Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Факультет информационной безопасности

Кафедра защиты информации

Т. В. Борботько, О. В. Бойправ

МЕТОДОЛОГИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. ПРАКТИКУМ

Рекомендовано УМО по образованию в области информатики и радиоэлектроники в качестве учебно-методического пособия для специальности 1-98 01 02 «Защита информации в телекоммуникациях»

Минск БГУИР 2024

УДК 004.056(076)
ББК 32.972.5я73
Б82

Р е ц е н з е н т ы:

кафедра телекоммуникационных систем учреждения образования
«Белорусская государственная академия связи»
(протокол № 9 от 21.03.2023);

ведущий научный сотрудник научно-исследовательской лаборатории
факультета связи и АСУ
учреждения образования «Военная академия Республики Беларусь»
кандидат технических наук, доцент А. В. Хижняк

Борботько, Т. В.

Б82 Методология информационной безопасности. Практикум : учеб.-метод. пособие / Т. В. Борботько, О. В. Бойправ. – Минск : БГУИР, 2024. – 60 с. : ил.
ISBN 978-985-543-745-2.

Содержит теоретические материалы и задания к практическим работам по дисциплине «Методология информационной безопасности».

УДК 004.056(076)
ББК 32.972.5я73

ISBN 978-985-543-745-2

СОДЕРЖАНИЕ

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 1:
«ОЦЕНКА ДОСТОВЕРНОСТИ ИНФОРМАЦИИ»

Цель занятия: изучить методику, позволяющую выполнить оценку достоверности информации, и получить практические навыки по ее применению.

Краткие теоретические сведения

Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления (*Закон Республики Беларусь № 455-З от 10.10.2008 «Об информации, информатизации и защите информации»*).

Информация необходима человеку для того, чтобы принять верное решение по тому или иному вопросу (сделать правильный выбор). Человек воспринимает информацию, используя различные органы чувств, основными из которых являются зрение и слух. Любой человек – часть общества и поэтому важным для него способом получения информации является коммуникация, в частности, вербальная (передача сведений с помощью речи) и невербальная (использование жестов, мимики, интонации и т. д.). Как правило, вербальная и невербальная коммуникации неразрывно связаны друг с другом.

Преобладание невербальной коммуникации у человека может быть обусловлено тем, что он плохо владеет языком, на котором осуществляется вербальная коммуникация (недостаточность словарного запаса и (или) неспособность его правильно применять), а также эмоциональным состоянием человека.

Эмоциональное состояние человека – психическое состояние, мотивирующее и регулирующее его деятельность (поведение, восприятие, мышление и т. д.), обусловленное его переживаниями и отношением в данный момент времени к окружающему миру, а также к себе лично.

Воспринимая информацию, человек аккумулирует ее в виде знаний, которые впоследствии могут быть использованы им для принятия решений. Многие люди хотели бы не ошибаться в жизни и принимать верные решения. Именно для этого им нужна достоверная (подлинная, неложная) информация.

Для принятия решения необходимо обладать достоверной и полной (подробной) информацией. Так, например, отправляясь в поездку на поезде, человеку необходимо знать не только дату и время отправления поезда, но и номер платформы и пути отправления.

Для того чтобы повлиять на принимаемое человеком решение, ему необходимо сообщить и внушить ложную информацию (дезинформацию). **Дезинформация** – ложные сведения, навязываемые одной стороной, участвующей в коммуникации, другой стороне, с целью введения ее в заблуждение и в конечном итоге принятия ею неверного решения.

Формирование, предоставление и навязывание дезинформации составляет суть информационного противоборства, что позволяет влиять на знания человека и на решение, которое он примет, в целом, используя накопленные

или полученные ранее им знания. **Информационное противоборство** – целенаправленное и планомерное информационно-психологическое воздействие на человека, группу людей или общество за счет использования таких способов предоставления информации, которые позволяют в значительной степени активизировать переживания и тем самым изменить психическое состояние и снизить активность применения критического мышления в процессе восприятия предоставляемой информации.

При восприятии информации человеком не последнюю роль играет его эмоциональное состояние (угнетенность, подъем, бодрость и т. д.). Поэтому для адекватного восприятия информации важным является наличие у человека критического мышления. **Критическое мышление** – способность человека, заключающаяся в проведении подробного анализа получаемой им информации за счет сопоставления анализируемых им сведений и накопленной ранее достоверной информации с целью выявления их несоответствия с последующим отвержением несоответствующих сведений.

Исходя из этого, важным процессом при усвоении некоторой информации является оценка ее достоверности. Проверка достоверности информации требует некоторого времени и является многостадийным процессом, в основу которого положен анализ содержания проверяемых сведений.

Методика оценки достоверности информации. Для выполнения оценки достоверности информации необходимо иметь непосредственно сведения, достоверность которых оценивается, а также их исходные данные (например, автор, источник, где они опубликованы, дата публикации и т. д.).

Учитывая то, что в создании информации непосредственное участие принимает человек, именно он является автором различных информационных сообщений, публикаций и т. д. Поэтому важным является доверие к автору информации, оцениваемой на достоверность.

На *первом этапе* методики выполняется именно такая проверка. Понимая сущность и тематику оцениваемой информации, необходимо обратить внимание на то, какие информационные сообщения были опубликованы этим автором ранее. Например, журналист, профессионал своего дела, всегда специализируется на определенной тематике. В процессе составления различных публикаций он постепенно обогащает свои знания и опыт по направлению специализации. Поэтому в его сообщениях в меньшей степени могут присутствовать сведения в виде оценки. Для уменьшения субъективизма в изложении материала такие журналисты прибегают к взаимодействию не с одним, а с несколькими экспертами для повышения объективности публикуемой информации. Это трудоемкий и длительный процесс, но он позволяет изложить материал более полно, с указанием конкретных фактов. С другой стороны, человек, который заинтересован в получении быстрого эффекта от публикации, навязывая определенное мнение, может излагать исключительно свою точку зрения или привлечь одного стороннего человека, обозначив его как эксперта по тематике сообщения. Такой подход минимизирует временные затраты при максимальном эффекте от сообщения, формируемого подобным образом.

Поэтому важно проанализировать следующие сведения об авторе сообщения (информации):

1. Фамилия, имя, отчество, адрес электронной почты, его статус (журналист, главный редактор и т. д.) в рамках данного информационного ресурса, агентства и т. д., его положение в обществе.

2. Какова репутация как автора, на чем он специализируется, является ли он экспертом по сути сообщения (сколько у него сообщений на подобную тему и каково их содержание, подробность изложения материала). Если после прочтения сообщения возникают вопросы и есть недосказанность, то всецело доверять автору сложно.

3. Ссылается ли он в сообщении на какие-либо источники и можно ли этим источникам доверять.

В любой стране мира доверие оказывается только официальным средствам массовой информации, которых не так и много. Например, в Республике Беларусь одно из старейших средств массовой информации – БелТА (Белорусское телеграфное агентство, основано в 1918 г.). Официальные источники информации всегда дорожат своей репутацией, поэтому сведения получают не у каких-то подписчиков, а напрямую у официальных лиц, которые делают соответствующие заявления и являются *первоисточником* информации. Необходимо понимать, что содержание некоторого текста, *пересказанное* разными людьми, по своей сути будет разное. Именно поэтому важным является получение сведений от их первоисточника.

Необходимо помнить, что чем меньше сведений можно собрать об авторе оцениваемой информации, тем более критически нужно относиться к ее содержанию.

На *втором этапе* выполняется анализ сведений об источнике информации (это может быть некоторое издание или электронный ресурс). Результатом данного этапа должно быть решение о том, можно ли доверять данному источнику информации.

Источники информации могут быть разнообразные: это средства массовой информации, которые аккредитованы в Республике Беларусь, это различные электронные ресурсы, информация, предоставляемая блогерами и поступающая через различные социальные медиа (сети), телеграм-каналы и т. д.

Гипотетически, чем больше ссылок на источник информации можно найти, тем выше доверие к источнику и транслируемой с его помощью информации. Вместе с тем необходимо помнить о том, что современные информационно-коммуникационные технологии позволяют достаточно быстро наращивать количество просмотров и организовывать множество ссылок на источник информации для того, чтобы создать *иллюзию* источника информации, которому можно доверять.

Репутация источника информации как достоверного формируется на протяжении *длительного времени*, поэтому необходимо представление о том, какое время существует этот источник. Необходимо помнить, что большое количество подписчиков не может являться критерием доверия к источни-

ку информации. Следует внимательно отнестись к «источникам-однодневкам», которые созданы незадолго до размещения оцениваемой на достоверность информации и могут быть использованы для распространения дезинформации.

Факты предоставляются следующими источниками: аккредитованными в Республике Беларусь средствами массовой информации (предоставление такими источниками ложных сведений приводит к отзыву лицензии и наступлению ответственности с учетом действующего законодательства), Национальным статистическим комитетом Республики Беларусь, научно-исследовательскими институтами. Если средство массовой информации предоставляет факты, но ссылки на источник отсутствует, то отнести такую информацию к достоверной сложно.

Например, сообщение следующего содержания: «Ученые установили, что для похудения необходимо каждое утро выпивать стакан молока» сложно считать фактом. В данном случае применяется отсылка к источнику информации «ученые», а фамилия, имя не указываются, что затрудняет оценку достоверности, и такое сообщение, скорее всего, будет отнесено к недостоверным или как минимум сомнительным.

Необходимо *внимательно относиться* к источникам информации, которые позиционируют себя как *независимые средства массовой информации*. Средству массовой информации нет необходимости заявлять или постоянно подчеркивать такой факт. Наличие подобных заявлений может быть типичной манипуляцией для привлечения внимания и навязывания дезинформации. Нужно помнить, что любой информационный ресурс требует определенных вложений от того юридического (организация) или физического (человек) лица, которое его поддерживает. Эти вложения в первую очередь финансовые (оплата электроэнергии, заработная плата сотрудников, оплата хостинга и т. д.). Поэтому любой из источников информации будет определенным способом финансироваться или в противном случае, спустя некоторое время прекратит свое существование, т. к. энтузиазм конечен ввиду снижения мотивации у человека с истечением времени.

На *третьем этапе*, прочитав и проанализировав сведения (например, публикацию в средствах массовой информации), необходимо вынести решение об отнесении содержания публикации к *факту* или *оценке*.

К *фактам* относят:

– свершившиеся события (дата рождения, дата окончания школы, дата зачисления в университет и др.), т. е. имеющие некоторое численное измерение, что позволяет их проверить;

– результат деятельности человека (построенный дом, спроектированное некоторое устройство и т. д.), который можно определенным образом осязать, и он измеряем в некотором численном эквиваленте (количество штук, геометрические размеры и т. д.).

К фактам относится все то, что поддается проверке (например, с помощью поисковых систем), измерению (например, с помощью измерительных

средств), подтверждению (например, с помощью каталогов и материалов архивов), осязанию (результат можно потрогать руками).

Оценка, в свою очередь, является субъективной точкой зрения даже тогда, когда отражает взгляд целой группы людей (информация может быть им навязана) или человека, которого считают или называют экспертом. Оценка может даваться на основании:

– эмоционального восприятия человеком окружающего мира (происходящих событий);

– личных предпочтений человека;

– определенных жизненных позиций и устоев человека;

– приобретенного ранее опыта и накопленных знаний.

Известная фраза древнегреческого философа Сократа гласит: «В споре рождается истина».

Оценка часто содержит *эмоциональную составляющую*, которая побуждает человека к действиям, мотивирует его выполнить что-либо, изменить свое мнение – это один из важнейших признаков. Для его обнаружения необходимо *внимательно* прочитать анализируемую информацию и постараться обнаружить фразы или предложения, которые позволяют влиять на эмоциональное состояние человека.

Важным является подтверждение фактов несколькими источниками информации, что позволяет проверить анализируемые сведения на достоверность.

На заключительном *четвертом этапе* выполняется анализ полноты информации. Недосказанность порождает ряд вопросов и если они возникают, то тогда вполне вероятно, что признать информацию полной будет сложно. При таком положении дел может сложиться так, что не все сообщение, но какую-то его часть можно признать полной. Предположим, у нас есть инструкция по пользованию, например, смартфоном, из которой удалили некоторые страницы. Оставшаяся в ней информация является достоверной, но не полной, т. к. она не позволит в полной мере обеспечить использование такого устройства. Именно поэтому, оценивая достоверность сведений, *важно* иметь представление об их полноте.

По итогу анализа оцениваемой информации может сложиться такая ситуация, что она не в полном объеме, а частично будет достоверной, именно эту часть сведений можно использовать в виде знаний и основания для дальнейшего принятия решения.

Задание

Выполнить оценку достоверности информации в соответствии с индивидуальным вариантом задания.

Контрольные вопросы

1. Что такое информация и зачем она нужна человеку?
2. Каким образом доверие к автору влияет на достоверность информации? Приведите пример.
3. Каким образом взаимосвязаны доверие к источнику информации и достоверность информации? Приведите пример.
4. Какие ключевые различия между оценкой и фактом? Назовите и поясните наиболее существенные из них.
5. По результатам проверки достоверности информации установлено, что только части сведений можно доверять. Опишите ваши дальнейшие действия.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 2: «КЛАССИФИКАЦИЯ ИНФОРМАЦИИ»

Цель занятия: изучить основные положения нормативных правовых актов, позволяющих классифицировать информацию, и получить практические навыки по их применению.

Краткие теоретические сведения

Взаимодействие людей друг с другом сопровождается обменом информацией (сведениями), которая используется человеком для принятия решений по различным вопросам, а также накапливается в виде знаний. Информация передается от одного человека к другому в процессе коммуникации. Выделяют вербальную и невербальную коммуникацию. **Вербальная коммуникация** – взаимодействие людей, построенное с использованием ими лексически выделенных единиц (слов). Такой вид коммуникации реализуется в устной (речевой) или письменной (текстовой) формах. **Невербальная коммуникация** – взаимодействие людей, построенное с использованием ими жестикуляции, мимики и т. д. в процессе вербальной коммуникации.

Выделяют следующие **формы представления информации**:

1. Бумажный документ – информация на бумажном носителе в виде символов (письменная речь) и изображений.

2. Электронный вид – информация, размещенная на физических носителях (жесткий диск, флеш-память и т. д.) в виде **файлов** (блок информации на запоминающем устройстве, имеющий определенное логическое представление и определенное имя в виде символов), которые могут содержать письменную и устную речь, а также изображения: подвижные (видеофильмы) и неподвижные (рисунки).

3. Физические поля – информация, распространяющаяся в соответствующей физической среде в виде сигналов (например, акустическая волна, электромагнитная волна).

Для обеспечения защиты информации необходимо обладать определенными ресурсами (наличие компетентных специалистов, финансовые средства, средства защиты информации и т. д.), которые независимо от масштаба организации *всегда ограничены*. Поэтому для эффективного и экономного использования ресурсов необходимо принять решение о том, какую информацию требуется защищать (определить перечень сведений, подлежащих защите), исходя из чего существующую в организации информацию необходимо классифицировать, т. е. из всего объема сведений нужно выделить те, которые подлежат защите.

Классификация информации выполняется специалистами по защите информации (т. е. теми людьми, которые эту защиту будут обеспечивать). Для этого используются нормативные правовые акты, которые устанавливают порядок обеспечения защиты информации. По результатам такой деятельности

специалист по защите информации составляет перечень сведений, подлежащих защите, который утверждается руководителем организации.

Одним из нормативных правовых актов, который используется при классификации информации, является ***Закон Республики Беларусь «Об информации, информатизации и защите информации» № 455-З от 10.11.2008 г.***

В соответствии с этим документом вся информация делится на две группы **(*Глава 3, Статья 15 Закона № 455-З*)**:

1. Общедоступная информация.

2. Информация, распространение и (или) предоставление которой ограничено.

В соответствии со ***Статьей 16 Закона № 455-З*** к общедоступной информации относится информация, доступ к которой, распространение и (или) предоставление которой *не ограничены*.

Доступ к информации – возможность получения информации и пользования ею.

Распространение информации – действия, направленные на ознакомление с информацией *неопределенного* круга лиц.

Предоставление информации – действия, направленные на ознакомление с информацией *определенного* круга лиц.

Необходимо отметить, что *предоставление информации* реализуется по запросу лица (человека) и в итоге этому лицу доступ может быть предоставлен или в доступе отказано в зависимости от того, имеет ли этот человек право доступа к интересующей его информации.

Рассмотрим пример. Предположим, есть паспортные данные некоторого человека: фамилия, имя, отчество, номер паспорта, срок его действия и дата выдачи, орган, который выдал этот паспорт, личный номер. У этого человека есть необходимость оформить кредит в банке (получение денежных средств). Одним из условий выдачи кредита банком является предоставление этим человеком его паспортных данных, т. к. кредит выдается на условиях платности (за пользованием деньгами банка придется платить) и возвратности (деньги необходимо вернуть к назначенному времени). Банк, получив паспортные данные человека, обязан ограничить к ним доступ (в том числе своих сотрудников), т. к. если эти сведения использует не их обладатель, то кредит (деньги) получит один человек (например, недобросовестный сотрудник банка), а возвращать деньги будет обязан тот, чьи паспортные данные были использованы при выдаче кредита. Именно поэтому важно ограничить доступ к такой информации.

Обладатель информации – субъект информационных отношений, получивший права обладателя информации по основаниям, установленным актами законодательства Республики Беларусь, или по договору.

Информационные отношения – отношения, возникающие при поиске, получении, передаче, сборе, обработке, накоплении, хранении, распространении и (или) предоставлении информации, пользовании информацией, защите информации, а также при применении информационных технологий.

Информационная технология – совокупность процессов, методов осуществления поиска, получения, передачи, сбора, обработки, накопления, хранения, распространения и (или) предоставления информации, а также пользования информацией и защиты информации.

В ***Статье 16 Закона № 455-З*** отмечено, что ***не ограничивается доступ***, а также распространение и (или) предоставление следующей информации:

– о правах, свободах, законных интересах и обязанностях физических лиц, правах, законных интересах и обязанностях юридических лиц и о порядке реализации прав, свобод и законных интересов, исполнения обязанностей;

– о деятельности государственных органов, общественных объединений;

– о правовом статусе государственных органов, за исключением информации, доступ к которой ограничен законодательными актами Республики Беларусь;

– о социально-экономическом развитии Республики Беларусь и ее административно-территориальных единиц;

– о чрезвычайных ситуациях, экологической, санитарно-эпидемиологической обстановке, гидрометеорологической и иной информации, отражающей состояние общественной безопасности;

– о состоянии здравоохранения, демографии, образования, культуры, сельского хозяйства;

– о состоянии преступности, а также о фактах нарушения законности;

– о льготах и компенсациях, предоставляемых государством физическим и юридическим лицам;

– о размерах золотого запаса;

– об обобщенных показателях по внешней задолженности;

– о состоянии здоровья должностных лиц, занимающих должности, включенные в перечень высших государственных должностей Республики Беларусь;

– накапливаемой в открытых фондах библиотек и архивов, информационных системах государственных органов, физических и юридических лиц, созданных (предназначенных) для информационного обслуживания физических лиц.

Таким образом, *Статья 16 Закона № 455-З* содержит перечень сведений, относящихся к *общедоступной информации*.

При классификации информации необходимо обратить внимание на ***Статью 17 Закона № 455-З***, которая содержит перечень сведений, ***распространение и (или) предоставление которых ограничено***:

– информация о частной жизни физического лица и персональные данные;

– сведения, составляющие государственные секреты;

– служебная информация ограниченного распространения;

– информация, составляющая коммерческую, профессиональную, банковскую и иную охраняемую законом тайну;

– информация, содержащаяся в делах об административных правонарушениях, материалах и уголовных делах органов уголовного преследования и суда до завершения производства по делу;

– иная информация, доступ к которой ограничен законодательными актами Республики Беларусь.

При составлении перечня сведений, которые подлежат защите, специалист по защите информации обязан использовать соответствующие нормативные правовые акты. Поэтому рассмотрим более подробно те категории сведений, которые требуют пояснений.

Первая категория информации, распространение и (или) предоставление которой ограничено – ***персональные данные***. Деятельность в области защиты персональных данных регламентируется ***Законом Республики Беларусь «О защите персональных данных» № 99-З от 07.05.2021 г.***

Персональные данные – любая информация, относящаяся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано.

Выделяют следующие ***виды персональных данных***:

– *биометрические* – информация, характеризующая физиологические и биологические особенности человека, которая используется для его уникальной идентификации (отпечатки пальцев рук, ладоней, радужная оболочка глаза, характеристики лица и его изображение и др.);

– *генетические* – информация, относящаяся к наследуемым либо приобретенным генетическим характеристикам человека, которая содержит уникальные данные о его физиологии либо здоровье и может быть выявлена, в частности, при исследовании его биологического образца;

– *специальные* – персональные данные, касающиеся расовой либо национальной принадлежности, политических взглядов, членства в профессиональных союзах, религиозных или других убеждений, здоровья или половой жизни, привлечения к административной или уголовной ответственности, а также биометрические и генетические персональные данные;

– *общедоступные* – персональные данные, распространенные самим субъектом персональных данных либо с его согласия, или распространенные в соответствии с требованиями законодательных актов.

Идентификация человека (физического лица) реализуется прямо (генетические персональные данные) или косвенно (общедоступные персональные данные) посредством анализа его персональных данных.

Физическое лицо, которое может быть идентифицировано – физическое лицо, которое может быть прямо или косвенно определено, в частности, через фамилию, собственное имя, отчество, дату рождения, идентификационный номер либо через один или несколько признаков, характерных для его физической, психологической, умственной, экономической, культурной или социальной идентичности

В соответствии со ***Статьей 17 Закона № 455-З*** вторая категория информации, распространение и (или) предоставление которой ограничено – ***государ-***

ственные секреты. Деятельность в области защиты государственных секретов регламентируется ***Законом Республики Беларусь «О государственных секретах» № 170-З от 19.07.2010 г.***

Государственные секреты (сведения, составляющие государственные секреты) – сведения, отнесенные в установленном порядке к государственным секретам, защищаемые государством в соответствии с настоящим *Законом* (*Законом Республики Беларусь № 170-З от 19.07.2010 г.*) и другими актами законодательства.

Сведения, которые могут быть отнесены к государственным секретам, определены в *Статье 14 Закона Республики Беларусь «О государственных секретах» № 170-З от 19.07.2010 г.* На документах, содержащих государственные секреты, проставляются следующие грифы секретности: «Особой важности», «Совершенно секретно» и «Секретно».

В соответствии со ***Статьей 17 Закона № 455-З*** третьей категорией информации, распространение и (или) предоставление которой ограничено, является ***служебная информация ограниченного распространения***. Сведения, относящиеся к такой категории информации, определены в ***Статье 18[1] Закона № 455-З***. Приведем выдержку из этой статьи.

Статья 18[1]. Служебная информация ограниченного распространения

К служебной информации ограниченного распространения относятся сведения, касающиеся деятельности государственного органа, юридического лица, распространение и (или) предоставление которых могут причинить вред национальной безопасности Республики Беларусь, общественному порядку, нравственности, правам, свободам и законным интересам физических лиц, в том числе их чести и достоинству, личной и семейной жизни, а также правам и законным интересам юридических лиц и которые *не отнесены к государственным секретам*.

Сведения относятся к служебной информации ограниченного распространения в соответствии с перечнем сведений, относящихся к служебной информации ограниченного распространения, определяемым Советом Министров Республики Беларусь, а также в случаях, предусмотренных законами Республики Беларусь и решениями Президента Республики Беларусь. Решение об отнесении сведений к служебной информации ограниченного распространения принимается руководителем государственного органа, юридического лица или уполномоченным им лицом.

На документах, содержащих служебную информацию ограниченного распространения, проставляется ограничительный гриф «Для служебного пользования».

Отнесение информации к этой категории выполняется в соответствии с ***Постановлением Совета Министров Республики Беларусь «О служебной информации ограниченного распространения» № 783 от 12.08.2014 г.***

В соответствии со ***Статьей 17 Закона № 455-З*** четвертой категорией информации, распространение и (или) предоставление которой ограничено, является ***информация, составляющая коммерческую, профессиональную, банковскую и иную охраняемую законом тайну***.

Правовая охрана коммерческой тайны регламентируется ***Законом Республики Беларусь «О коммерческой тайне» № 16-З от 05.01.2013 г.***

Коммерческая тайна – сведения любого характера (технического, производственного, организационного, коммерческого, финансового и иного), в том числе секреты производства (ноу-хау), соответствующие требованиям настоящего *Закона* (*Закон Республики Беларусь «О коммерческой тайне» № 16-З от 05.01.2013 г.*), в отношении которых установлен режим коммерческой тайны.

В соответствии со Статьей 5 этого закона режим ***коммерческой тайны*** может устанавливаться в отношении сведений, которые одновременно соответствуют следующим требованиям:

– не являются общеизвестными или легкодоступными третьим лицам в тех кругах, которые обычно имеют дело с подобного рода сведениями;

– имеют коммерческую ценность для их обладателя в силу неизвестности третьим лицам;

– не являются объектами исключительных прав на результаты интеллектуальной деятельности (исключительное право позволяет его обладателю распоряжаться результатом интеллектуальной деятельности);

– не отнесены в установленном порядке к государственным секретам.

Сведения имеют коммерческую ценность в случае, если обладание ими позволяет лицу при существующих или возможных обстоятельствах увеличить доходы, сократить расходы, сохранить положение на рынке товаров, работ или услуг либо получить иную коммерческую выгоду.

Обратите внимание на то, что необходимость отнесения сведений к информации, распространение и (или) предоставление которой ограничено (в данном случае коммерческой тайне), обусловлено ущербом, который может быть нанесен организации в случае ее разглашения.

Рассмотрим пример. Некоторой организацией объявлен тендер на закупку некоторого оборудования, и информация о технических характеристиках оборудования, которое требуется купить, размещена на специализированном сайте по закупкам. В тендере решили принять участие два поставщика. Они способны продать необходимую организации технику. Обе организации формируют свои предложения, в которых как у одного поставщика, так и у другого указана одинаковая техника. Для того чтобы выиграть тендер и получить деньги при продаже техники, необходимо каждому из поставщиков указать такую цену, которая бы покрыла его расходы и принесла прибыль, но в то же время была бы меньше, чем у поставщика-конкурента. Предположим, что первый поставщик определил эту цену и представил соответствующий документ организации, которая объявила тендер.

По просьбе второго поставщика один из сотрудников организации, в которую закупается оборудование, предоставил ему информацию о том, какую цену обозначил первый поставщик. На основании чего второй поставщик сформировал свое предложение по цене ниже, чем у первого поставщика. В случае если условия поставки у первого и второго поставщика одинаковы, то решение на закупку может быть принято по критерию наименьшей цены. Соответственно, первый поставщик проиграет тендер и не получит денежные средства, которые он рассчитывал получить при условии победы в тендере. Таким образом, неполученные средства можно рассматривать как ущерб, обусловленный недобросовестной конкуренцией второго поставщика, при участии сотрудника организации, объявившей тендер.

Проблема, изложенная в примере, могла бы быть решена, если бы в организации, объявившей тендер, приняли бы необходимые меры для ограничения доступа к информации, которая поступила от первого поставщика. Очень часто разглашение информации связано с тем, что классификация ее не выполнена и, соответственно, необходимые меры по ее защите не реализованы. Поэтому классификация информации – это первый шаг к обеспечению ее защиты.

Профессиональная тайна – общее наименование охраняемых законом тайн. Предметом профессиональной тайны является результат, который возникает в процессе взаимоотношений (трудовой деятельности) между нанимателем и работником определенной организации.

Правовой режим охраны *банковской тайны* регламентируется ***Банковским кодексом Республики Беларусь от 25.10.2000 г.***

В соответствии со Статьей 121 этого кодекса к ***банковской тайне*** *относятся* сведения о счетах и вкладах (депозитах), в том числе о наличии счета в банке (небанковской кредитно-финансовой организации), его владельце, номере и других реквизитах счета, размере средств, находящихся на счетах и во вкладах (депозитах), а равно сведения о конкретных сделках, об операциях без открытия счета, операциях по счетам и вкладам (депозитам), а также об имуществе, находящемся на хранении в банке.

Практическое задание

1. С использованием данных, приведенных в разделе «Краткие теоретические сведения», заполнить табл. 2.1.

2. Отнести информацию, наименования которой представлены в таблице, к одной из следующих групп:

а) информация об организации;

б) информация о внутренней деятельности организации;

в) информация о внешней деятельности организации.

Результат указать в графе «Вид информации» таблицы.

3. Указать категорию информации по каждому ее наименованию.

4. В графе «Примечания» указать ссылку на нормативный правовой акт, в соответствии с которым выполнялась классификация информации.

Таблица 2.1

Исходные данные для выполнения практического задания

Наименование информации	**Вид информации**	**Категория информации**	**Примечания**
Сведения о зарплате сотрудников организации			
Бухгалтерские отчеты организации			
Сведения о клиентах организации			
Сведения о партнерах и поставщиках организации			
График работы сотрудников организации			
Сведения о планах развития и расширения организации			
Сведения о прибыли организации			
Акты сдачи-приемки работ			
Личные дела сотрудников организации			
Сведения об экспорте и импорте вооружения и военной техники			
Сведения о технологии изготовления продукции, выпускаемой в организации			
Планы профориентационной работы организации			
Должностные инструкции сотрудников организации			
Перечень должностей, занимаемых сотрудниками организации			
ФИО сотрудников и данные о занимаемых ими должностях			
Биография руководителя организации			
Биография главного бухгалтера организации			
Договоры на выполнение работ и оказание услуг			

Окончание табл. 2.1

Наименование информации	Вид информации	Категория информации	Примечания
Перечень услуг, оказываемых организацией			
Структура административного управления организации			
Перечень приоритетных видов деятельности организации			
Информация о материально-технической базе организации			
Информация о системе специальной связи, используемой в организации			

Контрольные вопросы

1. Чем обусловлена необходимость классификации информации?
2. Каким образом выполняется классификация информации?
3. Что относится к информации, распространение и (или) предоставление которой ограничено?
4. В соответствии с какими нормативными правовыми актами выполняется классификация информации? Дайте пояснения по каждому нормативному правовому акту в части его использования при выполнения этой процедуры.
5. В чем отличие между предоставлением и распространением информации?

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 3:
«АНАЛИЗ ДЕМАСКИРУЮЩИХ ПРИЗНАКОВ ОБЪЕКТОВ»

Цель занятия: изучить классификацию демаскирующих признаков объектов и получить практические навыки по составлению уникальной совокупности признаков, которые позволяют идентифицировать заданный объект, используя эту классификацию; совершенствовать навыки проведения анализа сложных объектов.

Краткие теоретические сведения

Идентификация окружающих человека объектов (транспортные средства, объекты животного и растительного мира и т. д.) выполняется за счет анализа их признаков (демаскирующих признаков). Если совокупность демаскирующих признаков будет уникальна (не будет повторяться), то их можно использовать для идентификации объекта. Идентификация объекта позволяет установить его принадлежность к определенному классу, виду или типу.

Демаскирующие признаки – характеристики любого рода, поддающиеся обнаружению и анализу и являющиеся источником информации об объекте.

Таким образом, зная характеристики объекта, можно составить совокупность демаскирующих признаков (рис. 3.1), последующее использование которых позволит его идентифицировать среди объектов одного класса.

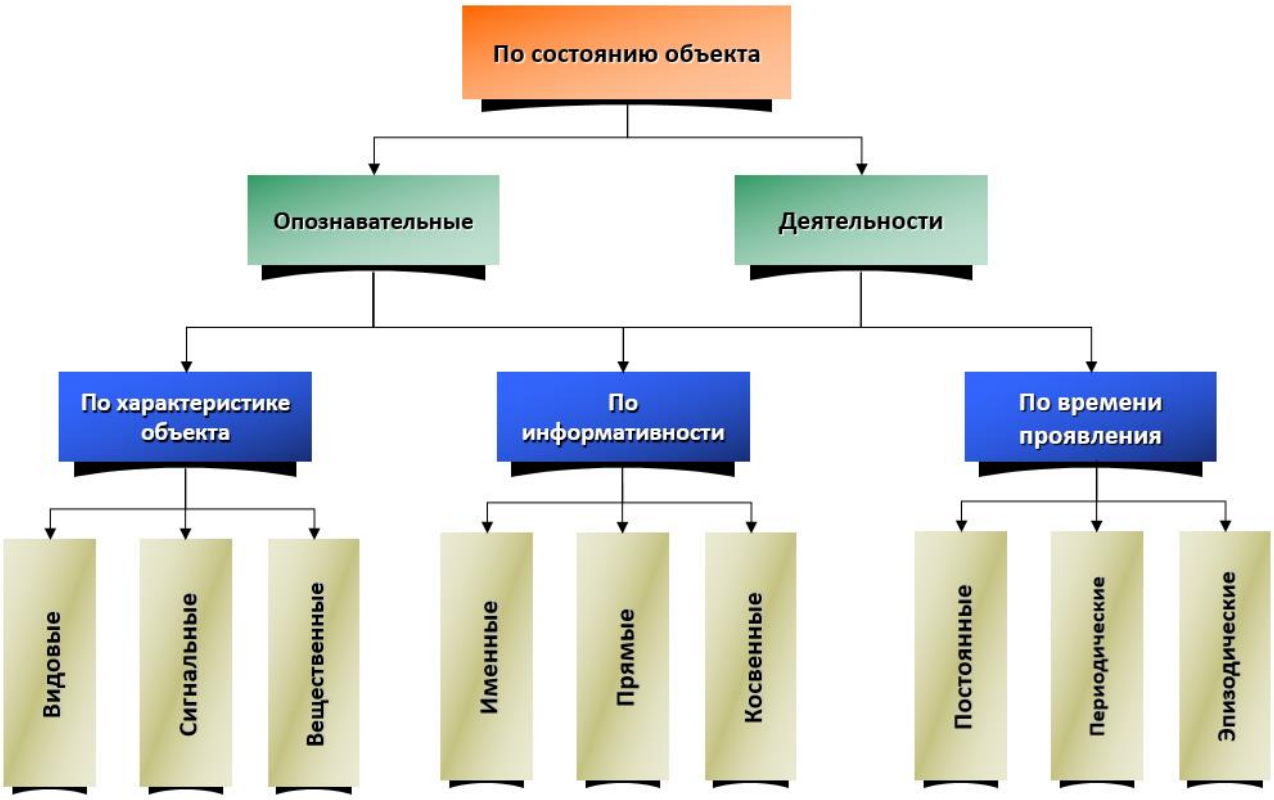


Рис. 3.1. Классификация демаскирующих признаков объекта

Опознавательные демаскирующие признаки характеризуют физические свойства объекта в статическом состоянии:

– внешний вид (цвет, форма, размер);

– физические свойства (масса, плотность, вязкость, проводимость);

– химические свойства (химический состав материала).

Демаскирующие признаки деятельности описывают последовательность событий во времени, или действий составных элементов объекта, или объекта в целом и взаимодействующих с ним других объектов, характеризуют этапы и режимы функционирования объекта (скорость, упругость ударов и т. д., т. е. изменения статистических свойств объекта во времени).

По характеристикам объекта демаскирующие признаки принято подразделять:

– *на видовые* (форма объекта, его размеры, детали объекта, тон, цвет, структура поверхности и т. д.);

– *сигнальные* (параметры физических полей и электрических сигналов, создаваемых объектом (амплитуда, частота, фаза, вид модуляции сигнала));

– *вещественные* (физический и химический состав, структура и свойства вещества, из которого состоит объект).

По информативности демаскирующие признаки делят:

– *на именные* (фамилия, имя, отчество человека, его биометрические характеристики, инвентарный номер прибора или мебели и т. д.). Главная отличительная особенность таких признаков – они обеспечивают вероятность идентификации объекта, близкую к 1 (значение вероятности изменяется от 0 до 1: значение вероятности 1 свидетельствует о том, что событие обязательно произойдет, а 0 – обязательно не произойдет). Поэтому в случае использования именных демаскирующих признаков ошибка идентификации объекта снижается;

– *прямые* (непосредственно принадлежащие определенному классу объекта. Вероятность идентификации объекта по такому признаку изменяется в пределах от 0 до 1) Так, например, у автомобиля есть кузов и колеса, а у человека – туловище, голова, руки и ноги;

– *косвенные* (непосредственно не принадлежащие объекту, но отражающие его свойства и состояние. Они позволяют повысить точность идентификации объекта). Например, по наличию тени, которая создается объектом, можно судить о его местоположении и даже форме.

В основу классификации заложен принцип оценки количества информации, которую можно получить в результате обнаружения демаскирующего признака объекта. Чем более уникален признак (чем меньше объектов реального мира им характеризуется), тем большую информативность он имеет. Наиболее информативны именные признаки – характерные только для конкретного типа объектов.

По времени проявления признаки разделяют:

– *на постоянные* (не изменяющиеся или незначительно изменяющиеся в течение жизненного цикла объекта);

– *периодические* (наблюдающиеся с определенной частотой (периодичностью));

– *эпизодические* (проявляющиеся при определенных условиях).

Рассмотрим изображение на рис. 3.2 и составим по нему совокупность демаскирующих признаков, используя их классификацию, представленную на рис. 3.1.

Рис. 3.2. Внешний вид некоторого объекта

Мы используем только изображение объекта, поэтому начнем его анализ с видовых демаскирующих признаков, т. к. для их формирования необходим внешний вид объекта.

К видовым демаскирующим признакам объекта относятся следующие его особенности: он имеет голову, туловище, руки и ноги. Необходимо отметить, что указанные видовые признаки по информативности относятся также к прямым демаскирующим признакам и свидетельствуют о том, что на изображении – представитель одного из классов животного мира. Форма этого объекта (взаимное расположение указанных его частей), которая также является видовым демаскирующим признаком, подтверждает то, что это человек.

Объект стоит на ногах – это косвенный демаскирующих признак, который подтверждает предположение о том, что это человек.

На туловище, части рук и на ногах у объекта надета одежда. В частности, штаны и футболка. Эти предметы одежды мы идентифицировали по их видовым демаскирующим признакам. Вместе с тем одежда – это косвенный демаскирующий признак того, что на изображении человек.

Все рассмотренные признаки, кроме положения объекта (стоит на ногах), являются постоянными. Именно поэтому можно идентифицировать объект. Это

однозначно человек. Как известно, человек может лежать и сидеть, поэтому текущее его положение в пространстве – это периодический демаскирующий признак.

Демаскирующие признаки, которые мы указали выше, относятся к опознавательным демаскирующим признакам, т. к. мы имеем дело со статическим объектом (неподвижным изображением). Если бы у нас был видеофильм, где был бы запечатлен человек в некотором движении, то мы смогли бы указать еще и признаки деятельности.

Вместе с тем в качестве демаскирующего признака деятельности человека можно отметить такой сигнальный демаскирующий признак, как речь.

Совокупность отмеченных выше демаскирующих признаков позволяет идентифицировать объект, в данном случае человека. Если бы нам необходимо было установить его личность, то это потребовало бы наличия уже именных демаскирующих признаков, которые на данном изображении отсутствуют.

Практическое задание

По изображению, выданному преподавателем, составить совокупность демаскирующих признаков объекта и выполнить процедуру его идентификации.

Контрольные вопросы

1. Что такое демаскирующие признаки объекта и на какие категории они делятся?
2. В чем заключается различие между опознавательными демаскирующими признаками и признаками деятельности объекта? Приведите пример для конкретного класса объекта.
3. Какие демаскирующие признаки объекта относятся к именным демаскирующим признакам и в чем отличие их от прямых демаскирующих признаков? Приведите пример для конкретного класса объекта.
4. Оцените значимость косвенных демаскирующих признаков при идентификации объекта.
5. При каких условиях можно составить демаскирующие признаки деятельности объекта?

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 4:
«АНАЛИЗ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ»

Цель занятия: изучить классификацию угроз безопасности информации, методику их оценки и получить практические навыки по ее применению для заданного объекта.

Краткие теоретические сведения

При доступе нарушителя к носителю информации происходит реализация угроз безопасности информации. Под **угрозой безопасности информации** будем понимать воздействия на носитель информации, которые приводят к ущербу. Для того чтобы понять, насколько та или иная угроза является существенной, оценивают ущерб, который причиняется вследствие ее реализации.

Ущерб может быть оценен в денежном эквиваленте (например, когда реализация угрозы разглашения данных платежной карточки приводит к потере денежных средств) или категориально (например, ущерб приемлем или ущерб неприемлем). Если человек принимает ущерб, то это означает, что текущая ситуация, складывающаяся в информационных отношениях, его устраивает.

Информационные отношения – отношения, возникающие при поиске, получении, передаче, сборе, обработке, накоплении, хранении, распространении и (или) предоставлении информации, пользовании информацией, защите информации, а также при применении информационных технологий.

Когда ущерб в денежном или категориальном исчислении неприемлем, то требуется обеспечить защиту информации, а точнее ее носителя для минимизации ущерба. Таким образом, необходимость обеспечения безопасности информации обуславливается необходимостью снижения ущерба от ее утраты.

Угрозы по их виду делят на следующие категории:

– угроза конфиденциальности – нарушение свойства информации быть известной только определенным субъектам информационных отношений (создатель, обладатель информации);

– угроза целостности – направлена на изменение содержания информации (искажение) или ее уничтожение;

– угроза доступности – приводит к нарушению доступа к информации, а также влияет на работоспособность ее носителя;

– угроза подлинности – приводит к невозможности однозначно идентифицировать (определить) ее автора или источник, из которого она получена;

– угроза сохранности – ее следствием является невозможность обеспечить такой режим хранения информации, который позволял бы гарантировать ее конфиденциальность, целостность и доступность.

Источниками угроз безопасности информации являются:

– человек – вследствие его целенаправленного (преднамеренного) или случайного воздействия на носитель информации;

– технические средства обработки информации – их некорректная работа или выход из строя приводят к различным видам угроз;

– программное обеспечение – ошибки в нем приводят к некорректной его работе и реализации различных видов угроз безопасности информации;

– внешняя среда – стихийные бедствия и другие воздействия на носитель информации, в том числе техногенного характера (отключение электропитания и т. д.), являются причиной реализации угроз безопасности информации.

По мере проявления угрозы безопасности информации делятся на преднамеренные и случайные угрозы.

Преднамеренные угрозы связаны с целенаправленными действиями человека и носят злонамеренный характер.

Случайные угрозы обусловлены недостаточной надежностью аппаратуры и программного обеспечения, воздействием внешней среды, а также незлонамеренными действиями человека в силу его некомпетентности или усталости.

Защита информации – комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации.

Различают следующие ***методы защиты информации***:

– *правовые* – определяют порядок регулирования информационных отношений и требования к средствам и системам защиты информации (нормативные правовые акты Республики Беларусь, приказы по организации и политике безопасности);

– *организационные* – регламентируют методы и способы достижения требований безопасности (изложенные в нормативных правовых актах) и позволяют повысить эффективность применения средств защиты информации;

– *технические* – обеспечивают конфиденциальность, целостность и доступность информации за счет использования криптографических и технических средств защиты информации.

Для того чтобы обеспечить безопасность информации, необходимо использовать правовые, организационные и технические методы. Их одновременное применение означает, что безопасность информации обеспечивается ***комплексно***.

Средства криптографической защиты информации – технические, программные, программно-аппаратные средства, которые реализуют криптографические алгоритмы и протоколы, а также функции управления криптографическими ключами, механизмы идентификации и аутентификации.

Средства технической защиты информации имеют техническую, программную или программно-аппаратную реализацию.

Необходимо отметить, что для того чтобы однозначно сказать, какие из угроз являются наиболее опасными, необходимо оценить ущерб от их реализации. Это позволит обосновать применение определенных методов и средств защиты информации.

Оценка угроз безопасности информации проводится в целях их идентификации для заданного объекта (носителя информации) и определения степени их

влияния на этот объект, что позволяет технически и экономически обосновать систему его защиты.

Оценка угроз безопасности информации должна носить систематический характер. Она проводится с использованием экспертного метода. Такой метод заключается в принятии решения экспертом – специалистом в определенной области (в данном случае в области информационной безопасности) на основании его опыта и знаний. Для снижения влияния субъективных факторов на результат оценки, она проводится группой экспертов.

При выполнении оценки угроз безопасности информации необходимо иметь полную информацию об объекте (его назначение, область применения, каким образом он задействован в информационных отношениях). На основании такой информации выполняется непосредственно оценка угроз для заданного объекта.

На *первом этапе* определяют, какие конкретно из угроз безопасности информации для данного объекта могут быть реализованы при доступе к нему нарушителя и к какому виду угроз они относятся.

Рассмотрим пример. Предположим, что текстовая информация, написанная от руки, относящаяся к информации, распространение и (или) предоставление которой ограничено, содержится на бумажном носителе, и этот носитель лежит на столе. Существует еще один аналогичный документ, который хранится в сейфе.

В случае доступа нарушителя к носителю реализуется угроза физического доступа к носителю информации, и она приводит к нарушению конфиденциальности информации, содержащейся на этом носителе, если нарушитель ее прочитает. При физическом доступе к носителю информации также возможна угроза доступности информации, т. к. нарушитель может уничтожить носитель. В рассматриваемом случае угроза целостности информации не является характе́рной, т. к. текст написан от руки и внесение любых изменений в существующий документ будет заметно. Для данного случая угроза подлинности также не является характе́рной. Вместе с тем, т. к. угрозы конфиденциальности и доступности возможны, это приведет также к реализации угрозы сохранности информации.

На *втором этапе* определяют негативные последствия, которые могут наступить вследствие реализации угроз безопасности информации и оценивают приемлемость ущерба вследствие их наступления.

Вернемся к рассмотренному выше примеру. По результатам первого этапа оценки угроз установлена возможность реализации угроз конфиденциальности и доступности информации для заданного объекта. Негативным последствием реализации угрозы конфиденциальности является разглашение сведений, которые содержатся на рассматриваемом носителе, т. к. они относятся к информации, распространение и (или) предоставление которой ограничено, и поэтому такой ущерб не является приемлемым.

Реализация угрозы доступности приведет к невозможности воспользоваться данным документом, но т. к. есть еще один, аналогичный по содержа-

нию, ущерб от этой угрозы приемлем. Исходя из вышеуказанного, т. к. ущерб от реализации угрозы конфиденциальности неприемлем, то и от реализации угрозы сохранности информации (см. определение) также будет неприемлем и поэтому его нужно минимизировать.

На *третьем этапе* выбирают методы и средства защиты, которые позволят минимизировать ущерб.

Закончим рассмотрение примера. На втором этапе было определено, что ущерб от угроз конфиденциальности и сохранности неприемлем. Так как возникновение угрозы сохранности обусловлено возникновением угрозы конфиденциальности, то, решая проблему конфиденциальности информации, можно решить и проблему ее сохранности. Минимизация ущерба может быть реализована за счет того, что мы ограничим доступ к бумажному носителю информации. Для этого его нужно со стола переместить в более надежное место, например, в сейф. В данном случае сейф будет являться средством защиты информации. Метод, который реализуется, – технический, т. к. сейф – техническое средство.

Как известно, безопасность информации требует комплексного решения проблемы. Поэтому для реализации правовых методов можно предложить разработку инструкции по работе с информацией на бумажных носителях, распространение и (или) предоставление которой ограничено. Эта инструкция будет определять порядок работы с бумажными носителями для того, чтобы минимизировать несанкционированный доступ к ним. В качестве организационных мероприятий необходимо обеспечить регулярную проверку (например, раз в неделю или месяц) выполнения положений этой инструкции.

По результатам оценки угроз безопасности информации оформим табл. 4.1.

Таблица 4.1

Результаты оценки угроз безопасности информации

Краткое описание защищаемого объекта	Угроза безопасности информации / вид угрозы безопасности информации	Возможные негативные последствия реализации угрозы	Ущерб (в случае приемлемости указать почему)	Метод защиты	Средство защиты или мероприятие
Информация в виде рукописного текста на бумажном носителе	Физический доступ к носителю информации / угроза конфиденциальности информации, угроза сохранности информации	Разглашение информации	Неприемлем	Технический	Сейф
				Организационный	Контроль соблюдения инструкции
				Правовой	Инструкция по работе с бумажными документами
	Физический доступ к носителю информации / угроза доступности информации	Уничтожение информации	Приемлем (есть носитель с аналогичной информацией)	–	–

Практическое задание

1. Оценить угрозы безопасности информации для следующих объектов:

– карта флеш-памяти с разъемом USB, которая содержит информацию, распространение и (или) предоставление которой ограничено; устройство хранится на столе; информация, записанная на устройстве, больше нигде не продублирована;

– персональный компьютер, подключенный к сети Интернет; на компьютере хранится информация, распространение и (или) предоставление которой ограничено; в информационной сети на сервере содержится резервная копия этой информации; компьютер стоит на столе в помещении;

– банковская карта, хранящаяся в тумбочке ее владельца; карта выпущена в одном экземпляре.

2. Результаты работы оформить в виде табл. 4.2.

Таблица 4.2

Результаты работы

Краткое описание защищаемого объекта	Угроза безопасности информации / вид угрозы безопасности информации	Возможные негативные последствия реализации угрозы	Ущерб (в случае приемлемости указать почему)	Метод защиты	Средство защиты или мероприятие

Контрольные вопросы

1. Что называется угрозой безопасности информации?
2. Поясните, в чем необходимость оценки ущерба при реализации угрозы безопасности информации?
3. Какие виды угроз безопасности информации вы знаете? Расскажите о каждом из них.
4. Для чего защищают информацию?
5. Зачем оценивают угрозы безопасности информации, и как это влияет на безопасность информации?

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 5: «ШИФРОВАНИЕ И РАСШИФРОВАНИЕ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ ШИФРА ЦЕЗАРЯ»

Цель занятия: изучение способов криптографического преобразования информации и получения базовых практических навыков шифрования сообщений, а также криптоанализа шифротекста на примере шифра Цезаря.

Краткие теоретические сведения

Взаимодействие двух субъектов информационных отношений обеспечивается посредством телекоммуникаций, поэтому передача сообщений от одного субъекта к другому реализуется по каналу связи. **Телекоммуникации** (от греческого tele – далеко, от латинского communicatio – общение) – комплекс технических средств, предназначенных для передачи информации на большое расстояние.

Для организации процесса перехвата информации, передаваемой по каналу связи, необходимо иметь доступ к физической среде передачи информации. В качестве такой среды выступают электрические и оптические кабели связи, воздушная среда. Процесс несанкционированного получения информации из канала связи называется **перехватом информации** (рис. 5.1).

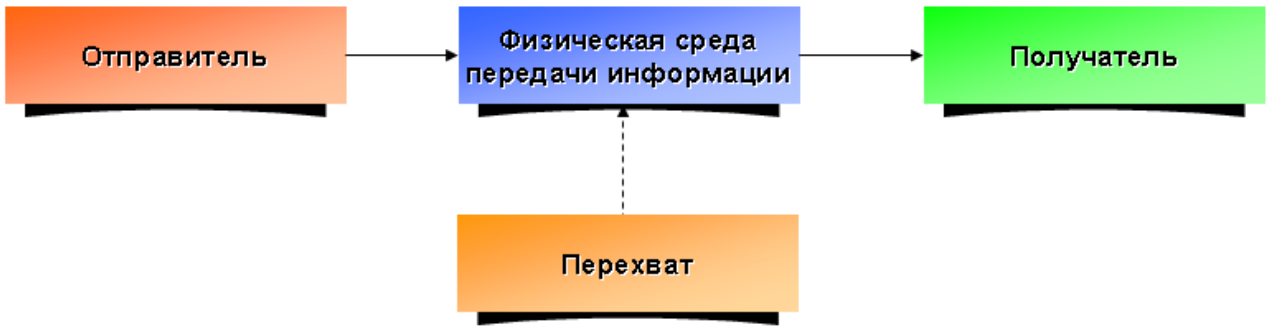


Рис. 5.1. Схематичное изображение перехвата информации в канале связи

Ввиду того что канал связи имеет значительную протяженность, обеспечить контроль физического доступа к нему является сложной организационно-технической проблемой. Поэтому для обеспечения безопасности информации, передаваемой по каналам связи, необходимо решить ряд задач:

– обеспечить ее конфиденциальность;
– обеспечить ее целостность;
– обеспечить ее подлинность;
– усложнить анализ потока сообщений.

Для решения таких задач используют криптографические методы защиты информации.

Криптография (от греческого kryptos – скрытый, grafo – пишу) – наука о методах, алгоритмах, программных и аппаратных средствах преобразования

информации в целях сокрытия ее содержания, предотвращения видоизменения или несанкционированного использования.

Информация, передаваемая по каналу связи и подлежащая шифрованию, называется **открытым (исходным) текстом** (обозначается латинской буквой *M* от английского *Message* – сообщение), а криптографически преобразованная информация называется **шифротекстом** (обозначается латинской буквой *C* от английского *Ciphertext* – шифротекст). Криптографическое преобразование открытого текста в шифротекст реализуется по некоторому алгоритму. Отправитель выполняет криптографическое преобразование (шифрование) открытого текста и формирует таким образом шифротекст, передавая его в канал связи, а получатель выполняет обратное криптографическое преобразование шифротекста (расшифрование) в открытый текст. Система, в которой осуществляется шифрование и расшифрование информации, называется **криптосистемой**, или **шифром**.

Нарушитель, получив доступ к физической среде передачи информации, перехватит шифротекст и будет выполнять его расшифрование для получения открытого текста. Расшифрование шифротекста будет успешным при условии, что нарушитель знает шифр. Для противодействия нарушителю при шифровании сообщений используется некоторый секрет, который называется криптографическим ключом. **Криптографический ключ** (обозначается латинской буквой *K* от английского *Key* – ключ) – информация, хранимая в секрете и используемая в криптосистемах. Стойкость любой криптографической системы определяется стойкостью используемого криптографического ключа. Необходимо выбрать не только определенную длину ключа, но и обеспечить режим секретности при его хранении и применении.

Исходя из особенностей применения криптографического ключа криптосистемы делят на симметричные и асимметричные. В симметричных криптосистемах для шифрования и расшифрования сообщений используют один и тот же криптографический ключ (рис.5.2).

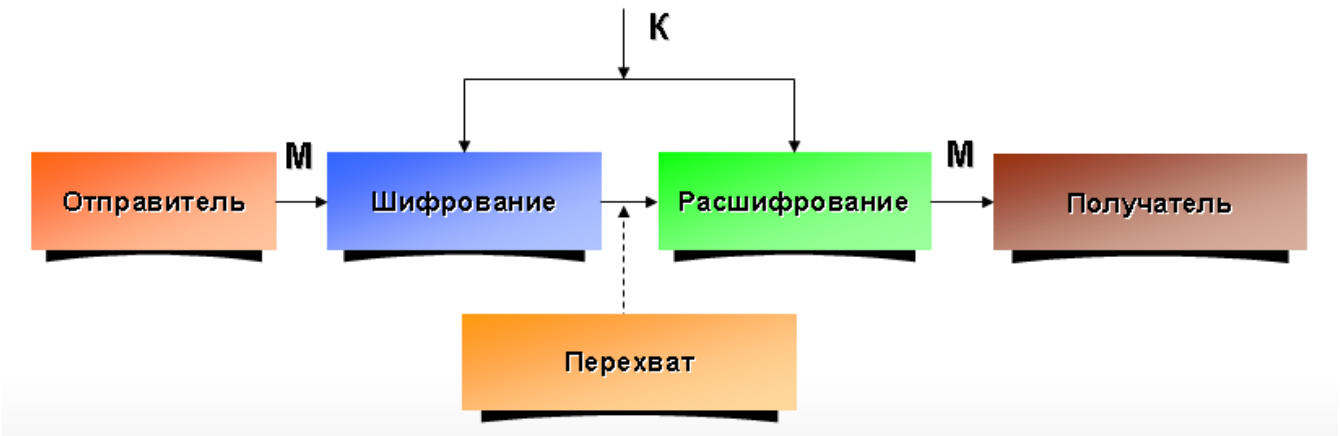


Рис. 5.2. Схематичное изображение симметричной криптосистемы

В криптографических системах одной из проблем является обмен криптографическими ключами между отправителем и получателем сообщений, для которого нельзя использовать канал связи, т. к. в канале связи всегда возможен перехват сообщений. Ключ может быть передан только при личном контакте отправителя и получателя сообщений.

В асимметричных криптосистемах (криптосистемах с открытым ключом) для шифрования сообщений используется один криптографический ключ (*K*1), а для расшифрования – другой (*K*2) (рис. 5.3). Такой подход упрощает процедуру обмена криптографическими ключами, т. к. отправитель информации получает ключ для ее шифрования (*K*1) от получателя по каналу связи, по которому впоследствии будет передаваться шифротекст. Передача криптографического ключа по каналу связи становится возможной, т. к. этот ключ позволяет только шифровать сообщение. Второй криптографический ключ (*K*2) используется получателем информации только для ее расшифрования и по каналу связи не передается.

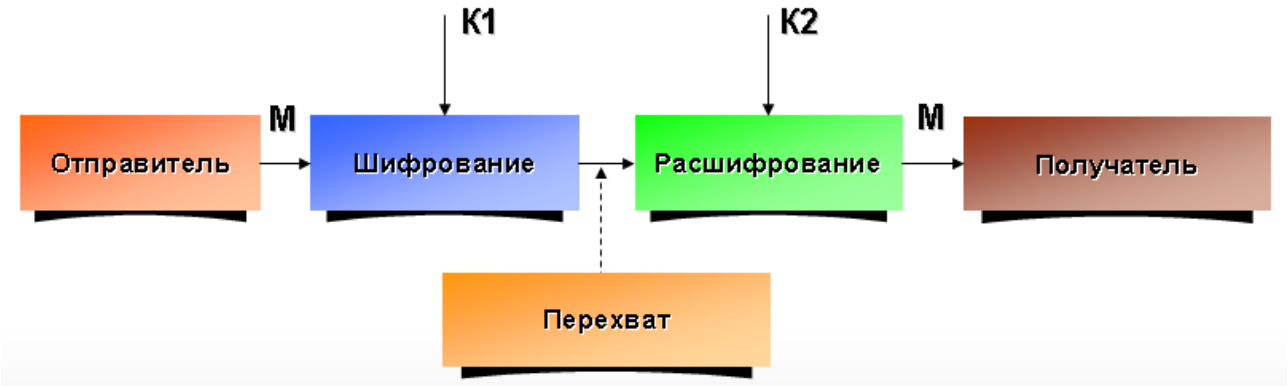


Рис. 5.3. Схематичное изображение асимметричной криптосистемы

В телекоммуникационных системах используют линейное (канальное) и абонентское шифрование информации. При линейном шифровании информации абонент (отправитель информации) формирует открытый текст и передает его на узел связи, где шифровальная аппаратура (аппаратно-программный комплекс для шифрования и расшифрования информации) выполняет криптографическое преобразование сообщения и передает шифротекст в канал связи. На приемном узле связи шифровальная аппаратура получает шифротекст и выполняет его расшифрование. При этом используются поточные шифры, и между узлами связи поддерживается постоянный поток шифротекста, непрерывность которого обеспечивается передачей пустых (незначащих) сообщений, что затрудняет анализ потока сообщений нарушителем. При таком способе связи нарушителю, для того чтобы получить открытый текст, будет необходимо получить доступ к узлу связи, т. к. на нем обрабатываются сообщения в открытом виде. Поэтому оба узла связи должны быть защищены от несанкционированного доступа.

Практическая реализация абонентского шифрования предполагает, что каждое сообщение шифруется в его источнике и расшифровывается только получателем. Сообщение, зашифрованное отправителем, может еще подвергаться и линейному шифрованию. Таким образом, абонентское шифрование обеспечивает конфиденциальность передаваемого сообщения, линейное – конфиденциальность и защиту сообщений от анализа. Успешный анализ шифротекста может привести к раскрытию криптографического ключа или получению открытого текста без знания криптографического ключа.

При абонентском шифровании за счет использования соответствующих режимов функционирования криптосистемы попутно решается и задача контроля целостности сообщения, а также проверки подлинности сообщения и его источника.

Шифр Цезаря – одна из самых простых и наиболее известных криптосистем, которая относится к шифрам подстановки. В этой криптосистеме каждый символ открытого текста заменяется символом, находящимся в алфавите на некотором постоянном числе позиций левее или правее заменяемого символа открытого текста. Число, характеризующее количество позиций сдвига влево или вправо по алфавиту относительно позиции преобразуемого символа открытого текста является криптографическим ключом и определяется выражением $n - 1$ (где n – число символов в алфавите).

Поэтому для шифрования информации необходимо иметь кроме открытого текста еще и алфавит. Рассмотрим пример шифрования сообщения, используя алфавит (рис. 5.4).

Зашифруем сообщение, в качестве которого используем слово «криптография». Для упрощения процедуры шифрования используем ключ $K = 10$. Так как мы шифруем сообщение, то сдвиг будем выполнять вправо. Первая буква в шифруемом сообщении «К». Для удобства шифрования буквы в алфавите пронумерованы. Порядковый номер буквы «К» – 12. Так как сдвиг выполняется вправо, то прибавим к числу 12 ключ 10. Получим число 22. Ему соответствует буква «Ф». Исходя из чего первая буква шифротекста – «Ф». Преобразование всех остальных букв сообщения выполняется аналогично. В итоге получится шифротекст «фътщьшмъйюти».

1 А	2 Б	3 В	4 Г	5 Д	6 Е	7 Ё	8 Ж	9 З	10 И	11 Й
12 К	13 Л	14 М	15 Н	16 О	17 П	18 Р	19 С	20 Т	21 У	22 Ф
23 Х	24 Ц	25 Ч	26 Ш	27 Щ	28 Ъ	29 Ы	30 Ь	31 Э	32 Ю	33 Я

Рис. 5.4. Алфавит

Для расшифрования шифротекста необходимо выполнить обратное его преобразование. Первая буква в шифротексте «Ф». Ее порядковый номер – 22. Необходимо из 22 вычесть значение криптографического ключа: 10. Получим 12 и, соответственно, букву «К».

Наука о раскрытии открытого текста зашифрованного сообщения без доступа к криптографическому ключу называется **криптоанализом**.

Понимая шифр Цезаря, можно выполнить криптоанализ шифротекста и, не зная криптографический ключ, вычислить его, а потом расшифровать весь шифротекст. Такую процедуру можно выполнить следующим образом. Необходимо взять шифротекст, например, «Уе йзфцк шцезе Уе шцезк йцфзе» и из него выбрать слово длиной порядка 5 букв. Перебирая все возможные значения криптографических ключей можно определить тот, при котором слово будет осмысленным.

Возьмем слово из шифротекста «йзфцк»:

1) ключ 1 – ижухй;
2) ключ 2 – зетфи;
3) ключ 3 – жесуз;
4) ключ 4 – едртж;
5) ключ 5 – егпсе;
6) ***ключ 6 – дворе.***

При криптографическом ключе, равном 6, мы получили слово «дворе». Криптографический ключ вычислен, можно расшифровать весь шифротекст.

«Уе йзфцк шцезе Уе шцезк йцфзе» – «На дворе трава На траве дрова».

Существуют и другие способы криптоанализа шифра Цезаря.

Практическое задание

1. Зашифровать сообщение в соответствии с индивидуальным заданием.
2. Расшифровать сообщение в соответствии с индивидуальным заданием.

Контрольные вопросы

1. Что называется перехватом информации?
2. Какое условие необходимо выполнить для организации процесса перехвата информации?
3. Какое наименование носит прямое и обратное криптографическое преобразование информации?
4. В чем особенности симметричной и асимметричной криптосистем?
5. Какие используются подходы для противодействия анализу потока сообщений?

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 6: «ОПРЕДЕЛЕНИЕ ПРИЗНАКОВ ФИШИНГА ПО СОДЕРЖАНИЮ СООБЩЕНИЙ ЭЛЕКТРОННОЙ ПОЧТЫ»

Цель занятия: изучить признаки фишинга содержащиеся в сообщениях электронной почты, и получить практические навыки их обнаружения в таких сообщениях.

Краткие теоретические сведения

Во многих организациях мира в основе обеспечения бизнес-процессов лежит применение электронной почты, которая позволяет передавать не только текстовые сообщения, но и различные файлы. Проверка подлинности сообщения, переданного по электронной почте на широко используемых почтовых ресурсах в корпоративных и глобальных информационных сетях, затруднительна. Для обеспечения безопасности информации, которая принимается, передается, обрабатывается и хранится в информационных системах, используются средства защиты информации, которые ограничивают к ней доступ посредством парольной защиты. Такое положение дел в информационных системах обуславливает проблему фишинга.

Фишинг (от английского *phishing* – выуживание идентификаторов, от английского *fishing* – рыбалка, выуживание) – способ получения нарушителем идентификаторов пользователя информационных систем (логин, пароль, данные платежной карты и т. д.), который основан на предоставлении пользователю такой информации и создании нарушителем таких условий ее восприятия, при которых пользователь примет ошибочное решение, в результате чего выполнит некоторое действие, которое является выгодным для нарушителя (передача идентификаторов, загрузка вредоносной программы).

Фишинг ориентирован на введение в заблуждение пользователя информационной системы, но его критическое мышление является барьером при принятии им ошибочного решения. Поэтому понимая, что в уравновешенном эмоциональном состоянии пользователь не может совершить необходимые нарушителю действия, нарушитель обязан изменить его эмоциональное состояние таким образом, чтобы нейтрализовать его критическое мышление на то время, когда он будет совершать выгодное для нарушителя действие. В этом заключается сущность *социальной инженерии* как методе управления действиями пользователя информационной системы.

Критическое мышление – способность человека, заключающаяся в проведении анализа получаемой им информации за счет сопоставления анализируемых им сведений и накопленной ранее достоверной информации с целью выявления их несоответствия с последующим отвержением несоответствующих сведений.

Фишинг делится на четыре вида.

1. *Почтовый* – сообщения, которые формирует нарушитель, передаются посредством электронной почты. Такие сообщения кроме текста содержат вложения в виде файла (рис. 6.1) или гипертекстовой ссылки на файл (рис. 6.2), загрузка которого или переход по которой приводит к загрузке и установке вредоносной программы на устройство пользователя (например, персональный компьютер, смартфон и т. д.).

Рис. 6.1. Фишинговое почтовое сообщение с вложенным файлом

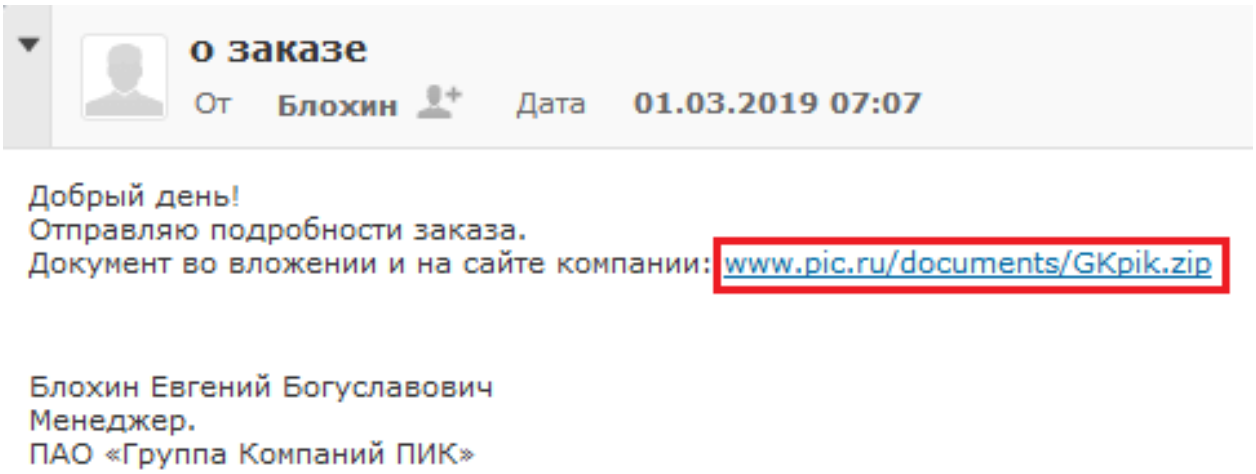


Рис. 6.2. Фишинговое почтовое сообщение с гипертекстовой ссылкой на файл

Почтовый фишинг приводит к несанкционированному доступу нарушителя к информационной системе, в результате которого могут произойти следующие события:

– выгрузка данных с устройства пользователя и при определенных условиях из информационной системы, куда его устройство подключено, для дальнейшей их продажи;

– получение всех идентификаторов учетных записей пользователя, которые он использует на данном устройстве;

– запуск вредоносной программы-шифровальщика с целью получения выкупа за расшифрование информации на данном устройстве.

2. *Онлайновый* – сообщения, которые формирует нарушитель, передаются посредством электронной почты и содержат кроме текста гипертекстовую ссылку или ссылку в виде «кнопки» (рис. 6.3), переход по которым приводит к загрузке сайта, контролируемого нарушителем, где пользователю будет предложено ввести свои идентификаторы (рис. 6.4).

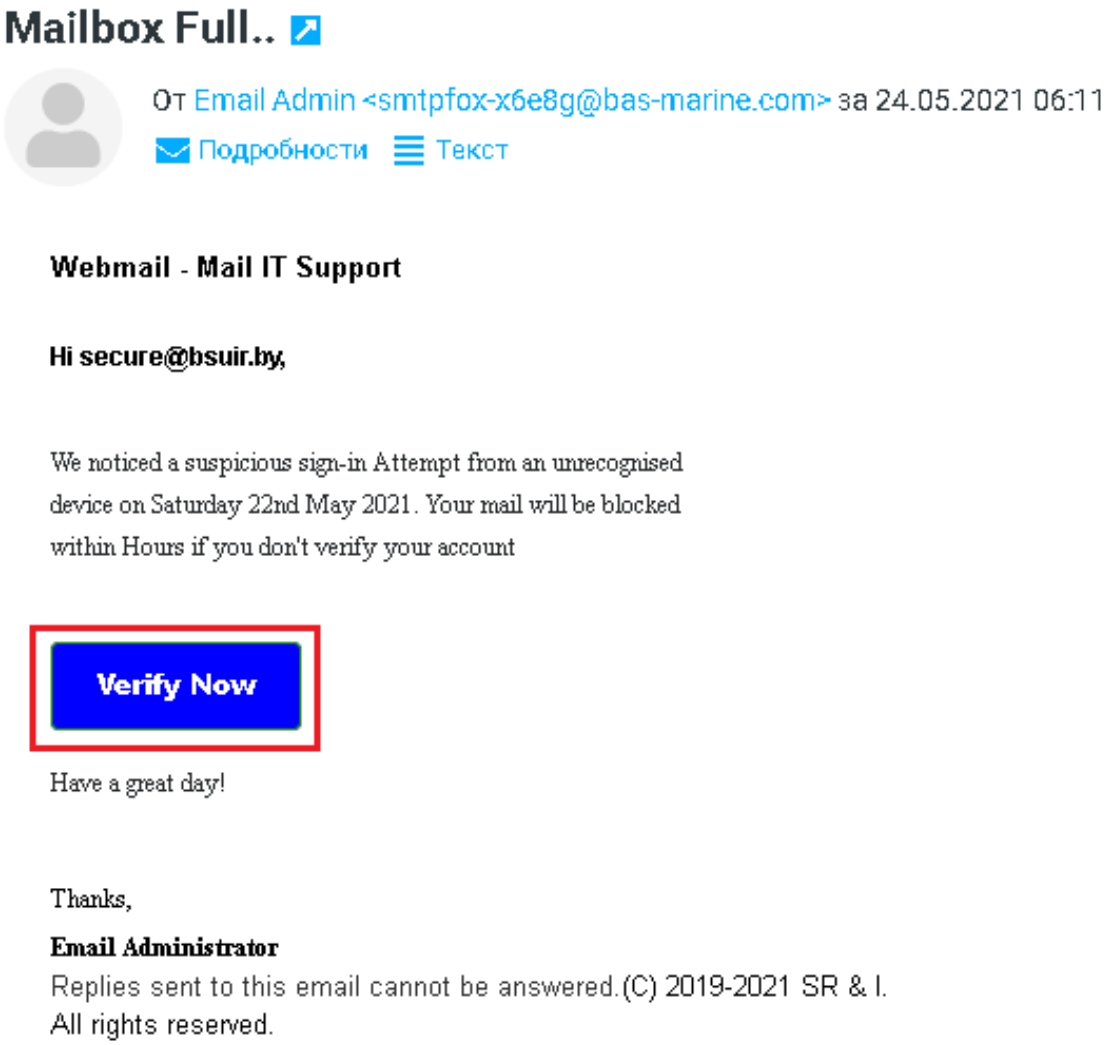


Рис. 6.3. Фишинговое почтовое сообщение со ссылкой в виде «кнопки»

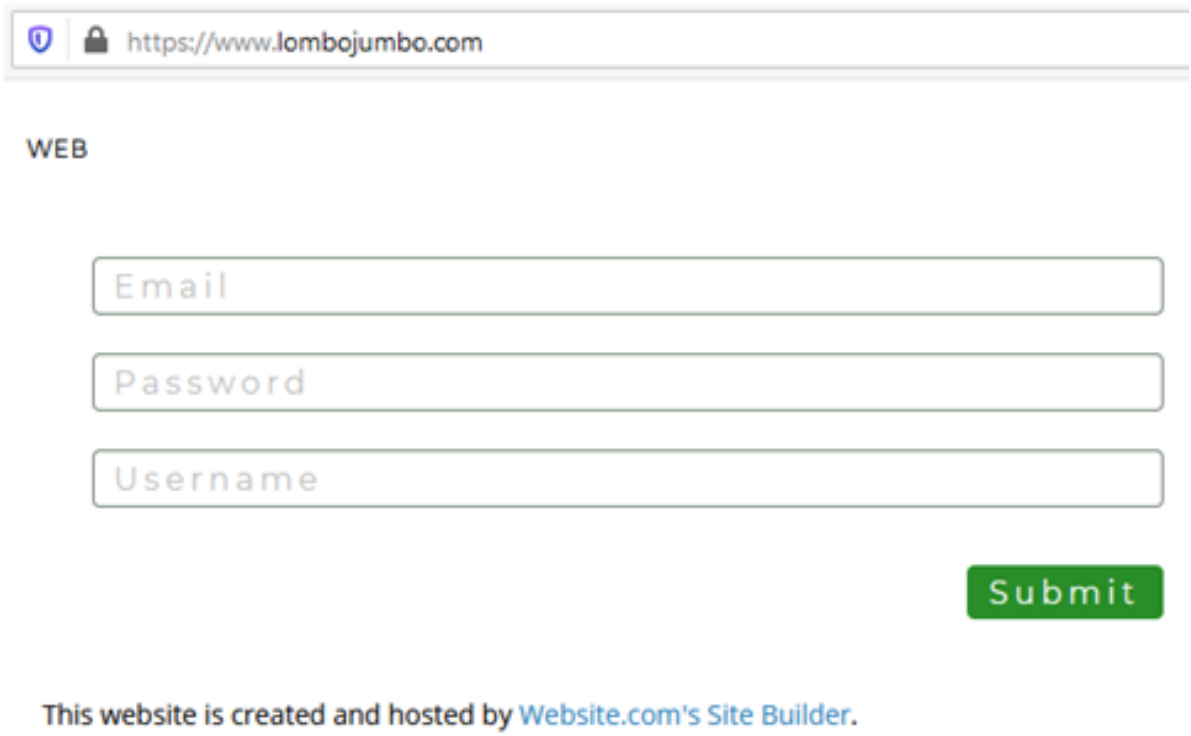
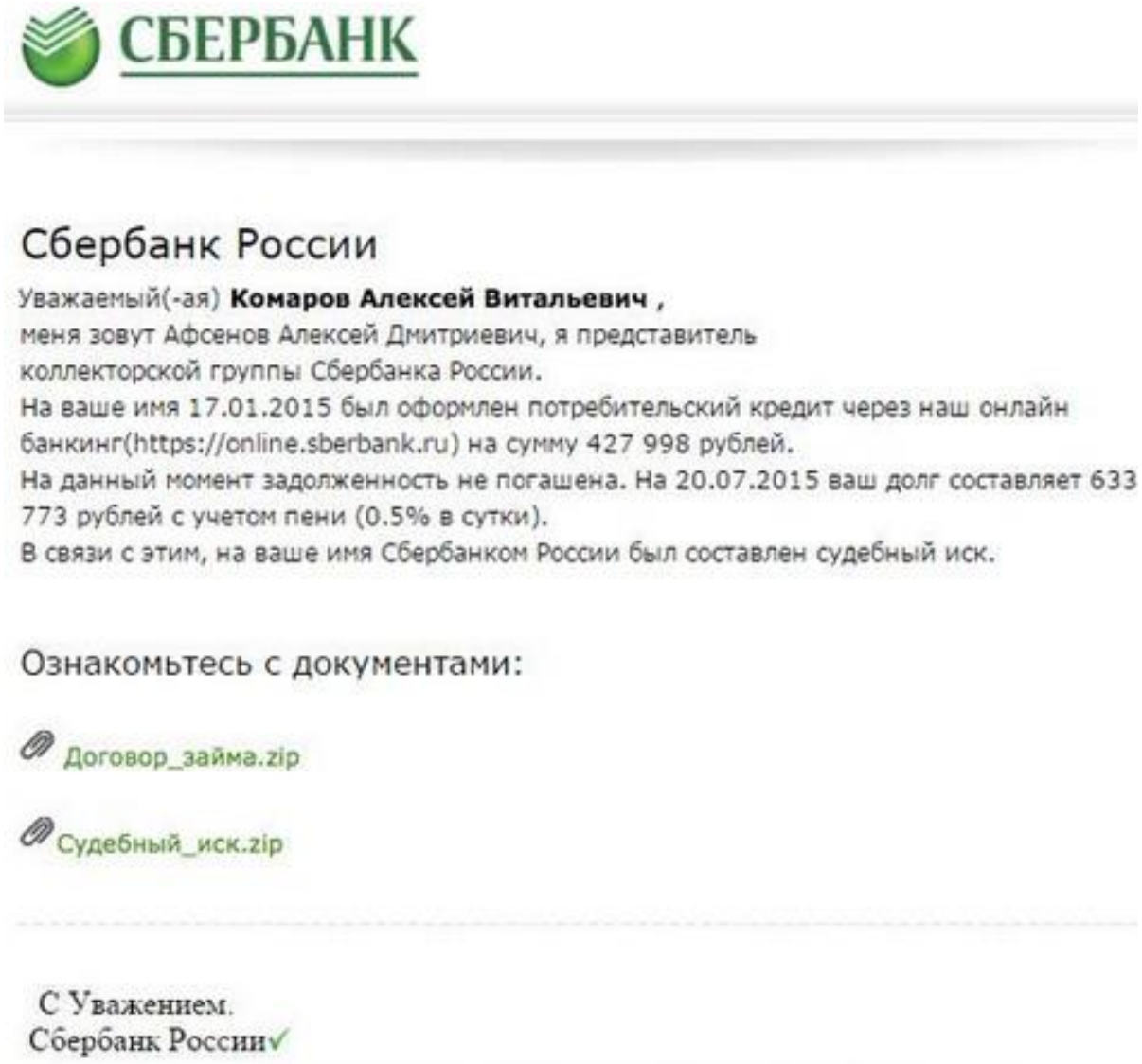


Рис. 6.4. Внешний вид фишингового сайта для сбора идентификаторов электронной почты

3. ***Спиарфишинг*** (от английского *spear* – гарпун; целенаправленный фишинг) – сообщения, которые формирует нарушитель, передаются посредством электронной почты. Их текст адресован конкретному человеку, т. к. нарушитель до составления такого сообщения смог получить доступ к персональным данным этого человека (рис. 6.5).

4. ***Вишинг*** – вид фишинга, реализуемый с помощью средств IP-телефонии (*IP – Internet Protocol*). В этом случае пользователь мессенджера получает на свой смартфон входящий голосовой вызов от нарушителя (рис. 6.6). Управление действиями пользователя по передаче идентификаторов нарушителю обеспечивается в процессе беседы с ним нарушителя. Этот вид фишинга ориентирован на получение денежных средств, поэтому нарушитель будет просить либо сообщить данные платежной карты, либо перевести деньги на его счет. Отличие вишинга от других видов фишинга заключается в том, что нарушитель будет стараться не дать человеку время на размышление о целесообразности того или иного действия. При почтовом же фишинге у пользователя электронной почты времени на обдуманное принятие решения больше.


СБЕРБАНК

Сбербанк России

Уважаемый(-ая) **Комаров Алексей Витальевич ,**
меня зовут Афсенов Алексей Дмитриевич, я представитель
коллекторской группы Сбербанка России.
На ваше имя 17.01.2015 был оформлен потребительский кредит через наш онлайн банкинг(https://online.sberbank.ru) на сумму 427 998 рублей.
На данный момент задолженность не погашена. На 20.07.2015 ваш долг составляет 633 773 рублей с учетом пени (0.5% в сутки).
В связи с этим, на ваше имя Сбербанком России был составлен судебный иск.

Ознакомьтесь с документами:

Договор_займа.zip

Судебный_иск.zip

С Уважением.
Сбербанк России✓

Рис. 6.5. Целенаправленное фишинговое почтовое сообщение
с вложенными файлами

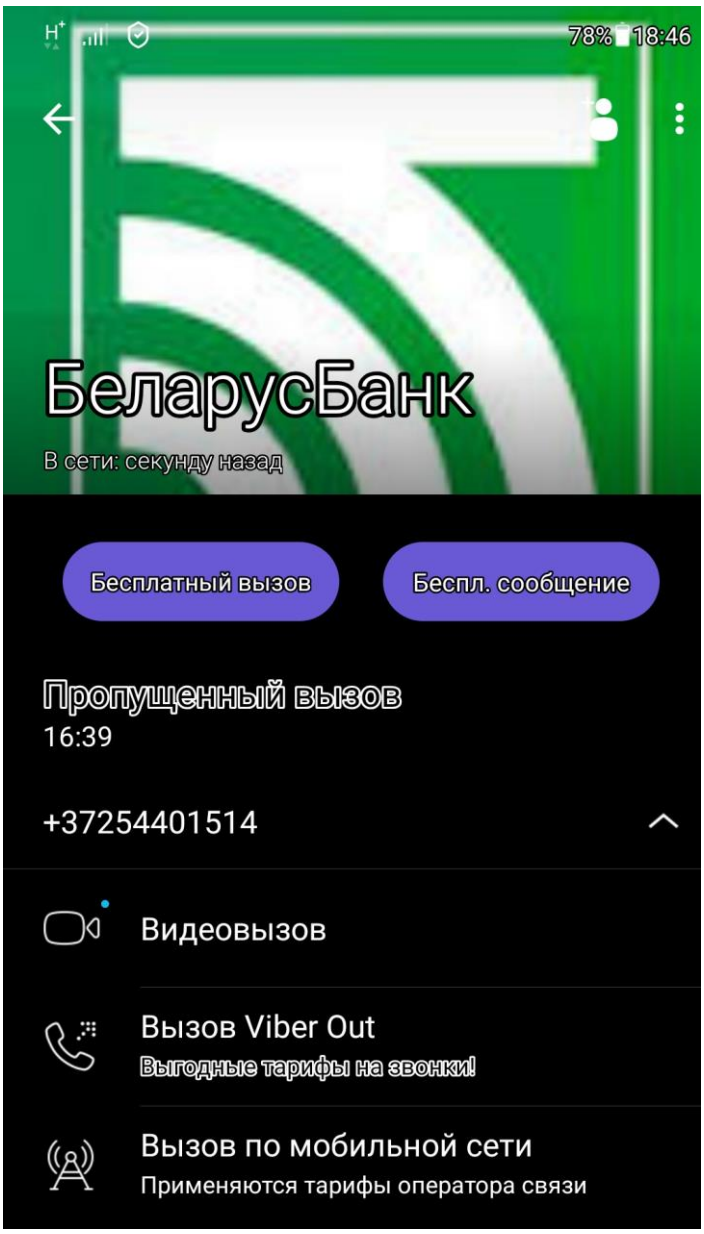


Рис. 6.6. Внешний вид окна мессенджера Viber с информацией о вызове, поступившем от нарушителя

Для изменения эмоционального состояния пользователя информационной системы нарушитель может использовать одну из следующих тактик.

1. Сообщить пользователю о некоторой существенной для него проблеме, и пока эмоциональное состояние человека не пришло в норму, предложить ему помощь в решении обозначенной проблемы (тактика «страха»). Суть «помощи» будет сводиться к завладению нарушителем идентификаторами пользователя. В данном случае на эмоциональное состояние человека воздействует страх. Пока он испуган – им можно управлять. Это классика фишинга, т. к. бесстрашных людей не бывает.

2. Сообщить человеку о радостной для него новости, например, что он выиграл крупную денежную сумму и может ее получить, но для этого необходимо, чтобы он сообщил идентификаторы своей банковской карты или оплатил

перевод «выигранных» денежных средств (рис. 6.7) (тактика «радости»). Получение внезапного подарка или приза всегда влияет на эмоциональное состояние человека, а также притупляет его критическое мышление. Подобная тактика является самой «древней» и носит наименование «нигерийских писем».

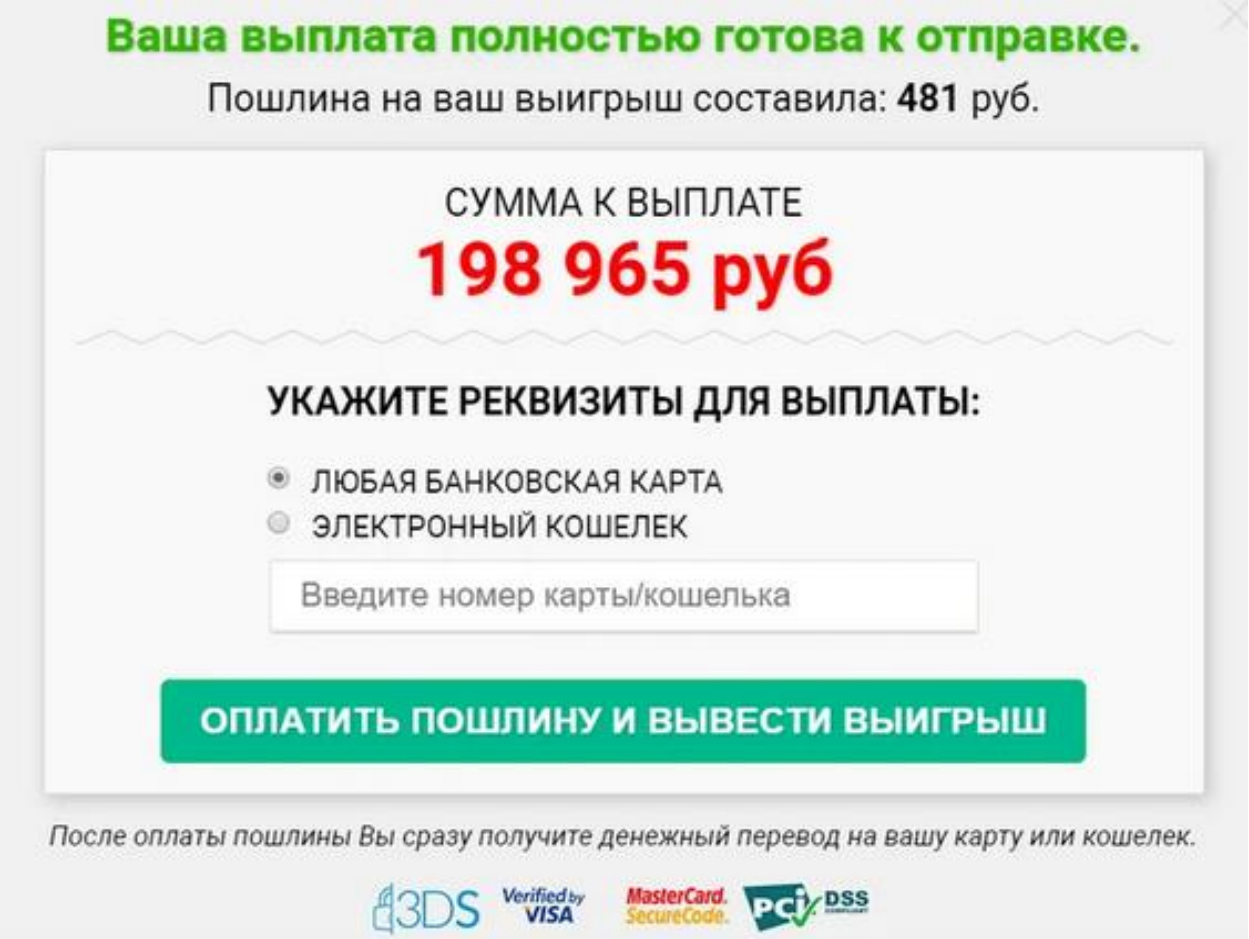


Рис. 6.7. Фишинговое почтовое сообщение о выигрыше

3. Послать сообщение пользователю электронной почты с некоторой интересной темой в надежде на его любопытство (тактика «любопытства»). Любознательность человека используется для эффективной реализации почтового фишинга. Грамотный выбор легенды сообщения (рис. 6.8) и массовая его рассылка могут дать возможность нарушителю скомпрометировать множество идентификаторов.

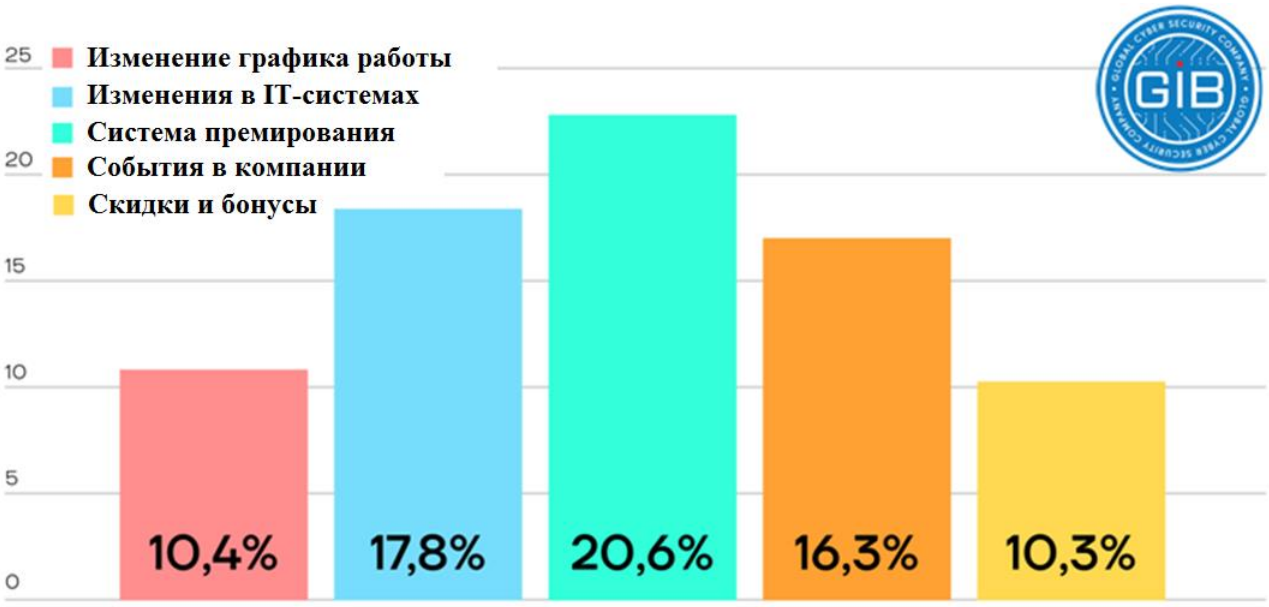


Рис. 6.8. Средняя результативность легенд сообщений электронной почты

Рассмотрим признаки фишинга, которые можно обнаружить при анализе сообщений электронной почты. К ним мы будет относить отклонение от нормального положения дел. Таким образом, суть анализа сообщений – это обнаружение аномалий.

1. Отправитель сообщения и время его отправления

Отправитель может быть известный или неизвестный (известных отправителей сложнее игнорировать). Время отправления сообщения может быть рабочее или нерабочее (деловая переписка в нерабочее время может быть аномалией, т. к. многие люди редко задерживаются на работе для выполнения своих должностных обязанностей, откладывая на завтра то, что не сделали сегодня).

2. Почтовый адрес отправителя сообщения

Необходимо обратить внимание на домен и наименование почтового ящика. Возможные аномалии: в результате анализа содержания сообщений делается вывод, что это деловая переписка, но для отправки сообщения используется не корпоративный домен электронной почты, а другие распространенные домены (например, mail.ru, gmail.com и т. д.). Наименование ящика электронной почты не содержит фамилии или имени отправителя сообщения (наличие фамилии, имени или инициалов в наименовании ящика – частый случай для корпоративной почты). Проверка принадлежности домена (наименование ящика после символа «@») может быть реализована путем его введения в URL-строку браузера. Это позволяет понять, какая электронная почта использовалась при отправке сообщения.

3. Текст сообщения и его оформление, тема сообщения

Текст сообщения должен отвечать требованиям деловой переписки не только по содержанию, но и по оформлению. Признаки деловой переписки:

– приветственное обращение по имени и отчеству к адресату;

– ФИО отправителя, его должность и некоторые реквизиты организации.

4. Тип вложения

Возможные аномалии:

– вложение является архивом (*.rar, *.zip);

– вложение – гипертекстовая ссылка;

– вложение имеет неизвестное расширение (*.001) или двойное расширение (*.docx.exe).

5. Наименование вложения

Возможная аномалия: наименование файла представляет собой написание русского слова в транслитерации (Oplata.zip, Dokumenti_dlia_proverki.001).

Проанализируем сообщение, пришедшее на электронную почту, и выделим признаки фишинга (рис. 6.9). Исходные данные для анализа сообщения:

1. Сообщение получено преподавателем БГУИР на его корпоративную электронную почту.

2. Университет имеет корпоративную почту в домене bsuir.by.

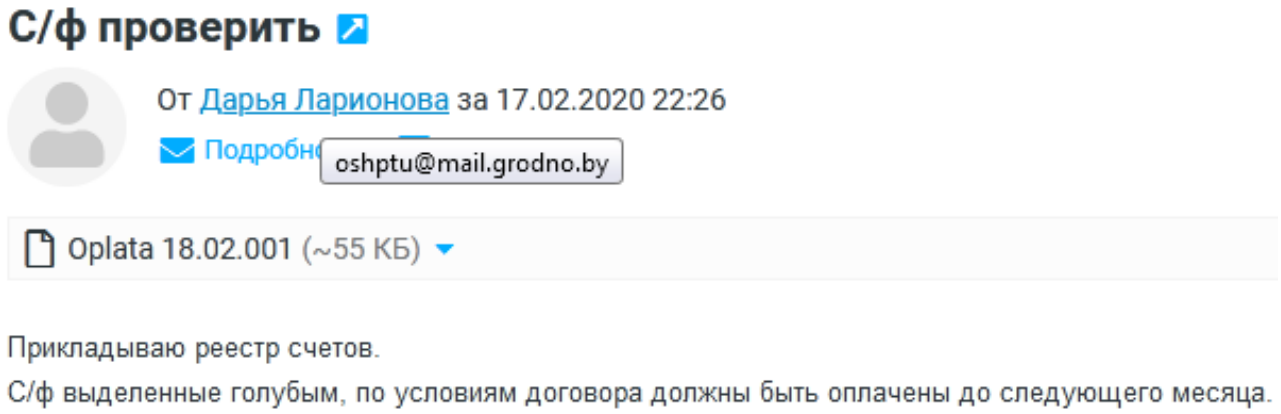


Рис. 6.9. Сообщение на электронной почте

1. Отправитель сообщения и время его отправления

Сообщение пришло от неизвестного преподавателю лица. Время отправки – нерабочее, хотя, судя по тексту сообщения, это деловая переписка. Так как сообщение пришло другому сотруднику, то в данном случае нарушителем используется тактика «любопытства». Если такое сообщение было бы доставлено сотруднику бухгалтерии, то речь шла бы о тактике «страха», ввиду того что оплата счетов не вовремя ведет к проблемам у человека, не выполнившего такую должностную обязанность. Это умозаключение подтверждается содержанием сообщения, потому что его текст имеет эмоциональную окраску, побуждающую получателя к действию.

2. Почтовый адрес отправителя сообщения

Почтовый адрес отправителя сообщения – «oshptu@mail.grodno.by». Наименование почтового ящика «oshptu» не имеет ничего общего с его отправителем «Дарьей Ларионовой». Домен, с которого отправлено письмо,

«*mail.grodno.by*» не имеет отношения к корпоративной почте конкретной организации. Этот сервис электронной почты предоставляется Белтелекомом, что подтверждается проверкой домена.

3. Текст сообщения и его оформление, тема сообщения

Текст сообщения имеет признаки деловой переписки, хотя в оформлении они отсутствуют. Тема письма – «С/ф проверить» – означает, что сообщение используется для пересылки счета-фактуры (сокращение «С/ф»). Преподаватель университета не является сотрудником бухгалтерии, поэтому счетами-фактурами он не занимается. Исходя из чего можно сделать вывод, что письмо пришло не по назначению. Кроме того, необходимо учесть, что случайностью пересылку сведений, относящихся к информации ограниченного распространения (счет-фактура), назвать сложно.

Признаки управления действиями получателя сообщения присутствуют. Они реализуются через осмысление текста сообщения. Так, например, для того чтобы оплатить счет-фактуру, нужно ее открыть (открыть файл). Открыть ее придется и для удовлетворения любопытства.

4. Тип вложения

К письму прикреплен файл, который имеет неизвестное расширение *.001, хотя речь идет о счете-фактуре, соответственно расширение файла должно соответствовать расширению, стандартному для документов данной категории.

5. Наименование вложения

Вложением является файл с русским наименованием, написанным в транслитерации: Oplata 18.02.

Вывод: данное сообщение является фишинговым. Открытие файла приведет к запуску и установке вредоносной программы. Сообщение необходимо удалить.

Практическое задание

1. Проанализировать сообщение (рис. 6.10), переданное по электронной почте, и определить признаки фишинга в нем.

2. Составить фишинговое сообщение с минимизированными признаками фишинга.

Исходные данные для анализа сообщения: сообщение получено преподавателем БГУИР на его адрес корпоративной электронной почты. Домен БГУИР – *bsuir.by*.

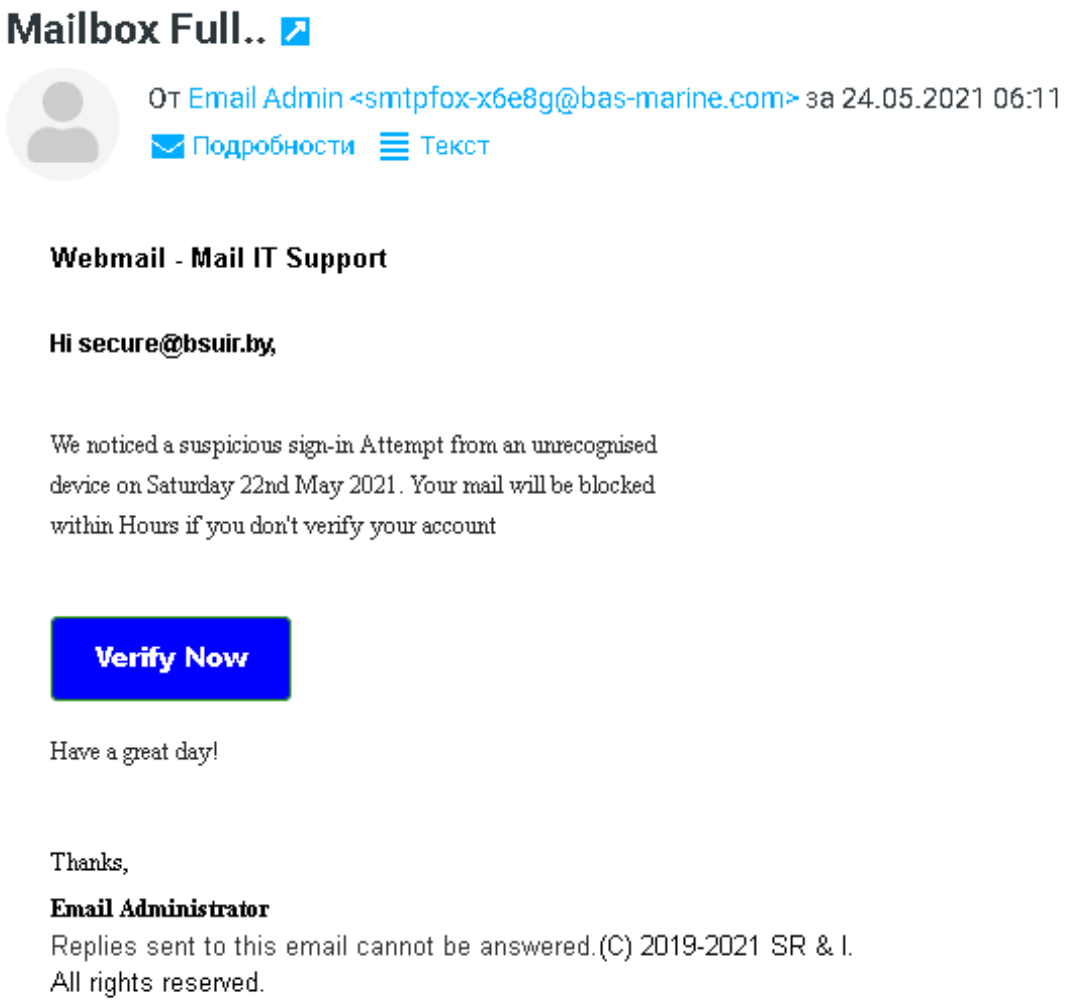


Рис. 6.10. Сообщение, пришедшее на электронную почту

Контрольные вопросы

1. На чем основан фишинг?
2. В чем заключается сущность социальной инженерии?
3. Какой из видов фишинга наиболее опасный? Обоснуйте ответ.
4. Какой из видов фишинга наиболее эффективный для нарушителя? Обоснуйте ответ.
5. Какой из признаков фишинга наиболее оптимальный для обнаружения подобных сообщений? Обоснуйте ответ.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 7: «ОЦЕНКА СТОЙКОСТИ ПАРОЛЬНОЙ ЗАЩИТЫ ДАННЫХ»

Цель занятия: изучение особенностей построения систем парольной защиты данных информационных систем, требований, предъявляемых к паролю, и получение практических навыков оценки стойкости парольной защиты данных.

Краткие теоретические сведения

Информация, распространение и (или) предоставление которой ограничено, как известно, подлежит защите. Такая информация обрабатывается в информационных системах.

Информационная система – совокупность *банков данных*, информационных технологий и комплекса (комплексов) программно-технических средств.

Банк данных – организационно-техническая система, включающая одну или несколько *баз данных* и систему управления ими.

База данных – совокупность структурированной и взаимосвязанной информации, организованной по определенным правилам на материальных носителях.

Для контроля доступа пользователей информационной системы к такой информации необходимо выполнить проверку прав доступа пользователя (субъекта доступа) и на основании наличия или отсутствия таких прав принять решение: разрешить или запретить им доступ к информации. Система, которая реализует такую процедуру, называется **системой авторизации пользователей**.

Авторизация – предоставление прав доступа субъекту доступа к информации, обрабатываемой в информационной системе.

Любую информационную систему можно представить как совокупность субъектов и объектов и отношений между ними (рис. 7.1). **Объект** – пассивный компонент системы, который хранит в себе информацию (примером такого объекта является файл). **Файл** – структурированная по определенным правилам информация, представляющая собой блок данных, имеющий определенное наименование (имя). **Субъект** – активный компонент системы, который, получая доступ к объектам системы, обуславливает поток информации от одного объекта к другому (например, копирование информации из одного файла в другой).

Рис. 7.1. Схематичное изображение компонентов информационной системы

Субъектом в информационной системе является человек, но он непосредственно не взаимодействует с объектами (файлами), т. к. они не могут быть непосредственно им прочитаны, как, например, информация, содержащаяся на бумаге. Поэтому человеку необходимо использовать соответствующие программно-технические средства, которые предоставят ему информацию, содержащуюся в объектах (файлах) в таком виде, который он сможет воспринимать. Именно поэтому **субъектом доступа** в информационной системе является не человек, а программно-технический комплекс (например, персональный компьютер), с помощью которого человек осуществляет доступ к информационной системе и информации хранимой в ней.

В рамках информационных систем информация хранится в виде файлов, размещаемых на машинных носителях. Субъект доступа может получить следующие ***права доступа*** к информации (файлам):

– *чтение* – позволяет открыть файл и ознакомиться с его содержанием (применимо к текстовым и исполняемым файлам);

– *запись* – позволяет открыть файл, ознакомиться с его содержанием и изменить его (применимо к текстовым и исполняемым файлам);

– *исполнение* – позволяет выполнить код, содержащийся в этом файле (применимо к исполняемым файлам).

Для того чтобы можно было провести авторизацию пользователя информационной системы, необходимо каким-то образом его опознать. Для этого существует процедура идентификации.

Идентификация – процесс присвоения уникального (неповторимого) признака (идентификатора) субъекту доступа, по которому он впоследствии будет опознан.

Выделяют следующие **виды идентификаторов**:

1. Идентификатор, который известен только субъекту доступа. Такой подход предполагает, что идентификатор необходимо запомнить. Примером является пароль.

2. Идентификатор может быть записан на некоторое устройство, которое гарантирует противодействие угрозе сохранности идентификатора. Примером являются специализированные устройства, обеспечивающие сохранность информации и подключаемые к персональному компьютеру через разъем *USB*. Они имеют внешнее сходство с картой флеш-памяти, которая имеет разъем *USB*. Применение таких идентификаторов сопряжено с проблемами, связанными с потерей таких устройств (человек, нашедший такое устройство, сможет с его помощью авторизоваться от имени владельца устройства), и случаями, когда такие устройства владелец забывает отключить от персонального компьютера и оставляет без контроля (человек, который получит физический доступ к такому компьютеру, сможет авторизоваться от имени владельца).

3. В качестве идентификатора могут быть использованы биометрические характеристики человека (поведенческие и физиологические). Использование таких идентификаторов сопряжено с ошибками идентификации, которые обусловлены тем, что эти характеристики варьируются в течение суток в некоторых пределах, т. к. человек является живым объектом. Кроме того, если к такому идентификатору получит доступ нарушитель и скопирует его, то изменить такой идентификатор у владельца не получится, в отличие, например, от обычного пароля.

В информационных системах наиболее широко используют такой идентификатор, как пароль. Это обусловлено рядом его ***преимуществ***:

– выбрать его может сам пользователь информационной системы;

– при компрометации его можно достаточно легко сменить;

– сложность и стоимость системы невысока.

Таким образом, процедура идентификации пользователя (субъекта доступа) заключается в выдаче пользователю уникального идентификатора. Для того чтобы субъект доступа получил доступ к информации, необходимо реализовать еще одну процедуру – процедуру аутентификации. **Аутентификация** – процесс проверки подлинности субъекта доступа по его идентификатору.

Система, реализующая контроль доступа к ней по паролю, состоит из ***трех основных компонентов*** (рис. 7.2):

1. Рабочее место пользователя (например, персональный компьютер), на котором установлено прикладное программное обеспечение (например, браузер). Такое рабочее место в терминологии компьютерных сетей называется клиентом.

2. Сервер, который способен принять запрос от субъекта доступа и по предоставленной ему информации проверить его подлинность.

3. База данных и система управления ею. База данных хранит идентификаторы всех зарегистрированных в информационной системе субъектов доступа.

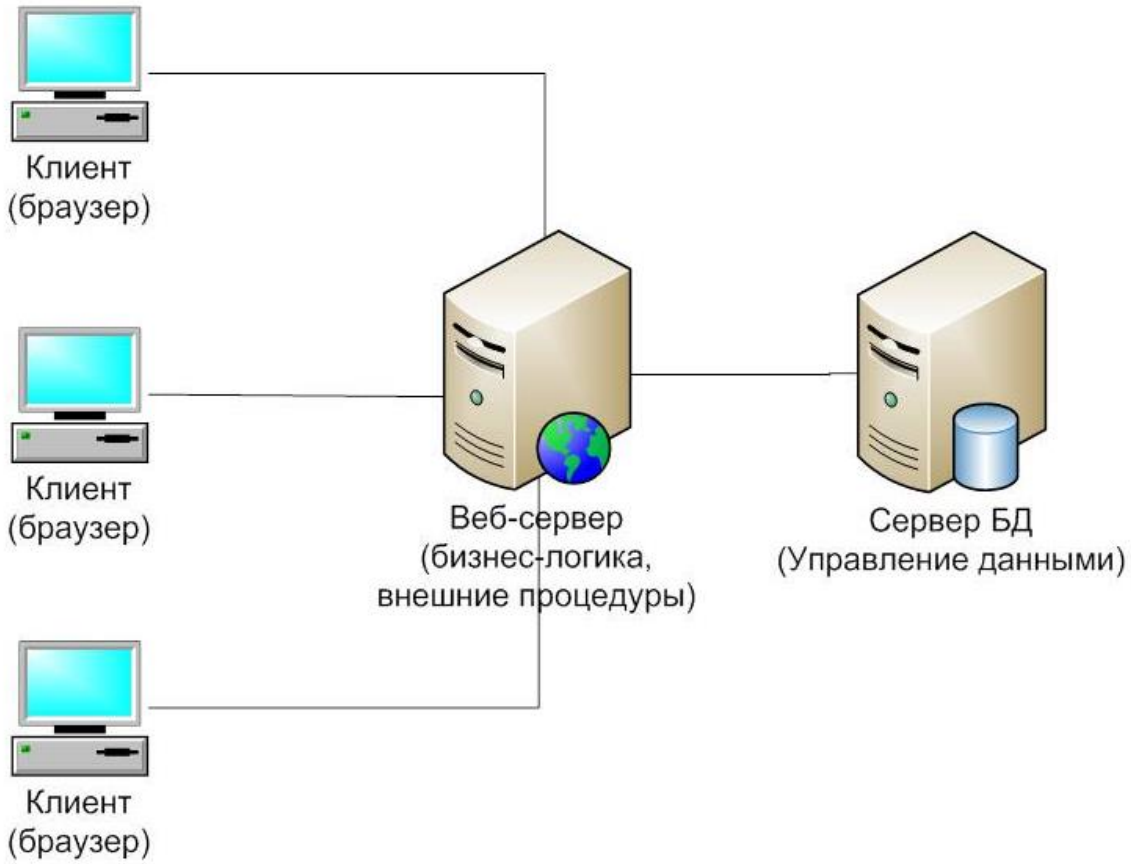


Рис. 7.2. Схематичное изображение информационной системы, реализующей функцию аутентификации субъекта доступа

Аутентификация субъекта доступа происходит по следующей схеме. Субъект доступа подключается к информационной системе, и та ему предлагает ввести логин и пароль (идентификатор), демонстрируя окно авторизации (рис. 7.3). Человек вводит логин и пароль. Браузер передает эти данные веб-серверу, который, получив их, формирует запрос к системе управления сервера баз данных (БД). Система управления, получив логин и пароль пользователя, анализирует содержимое базы данных на предмет наличия такого идентификатора. В случае если он найден в базе данных, то система управления базой данных передает на веб-сервер информацию, что результат аутентификации пользователя положительный, и пользователь получит доступ к массиву данных, в противном случае в доступе субъекту доступа будет отказано.

Рис. 7.3. Внешний вид окна авторизации

Система парольной защиты – программно-аппаратный комплекс, реализующий на основе одноразовых или многоразовых паролей процессы идентификации, аутентификации и авторизации субъектов доступа информационной системы.

Пароль пользователя – информация, известная только пользователю и хранимая в парольной системе, которая должна сохраняться в секрете и может быть предъявлена пользователем для прохождения процедуры аутентификации. Одноразовый пароль дает возможность субъекту доступа однократно пройти аутентификацию, после чего пароль аннулируется. Многоразовый пароль может быть использован для проверки подлинности субъекта доступа повторно.

Совокупность логина и пароля пользователя образуют его **учетную запись**.

Рассмотрим ***основные пути реализации угроз*** в отношении систем парольной защиты.

1. Определение параметров учетной записи через:

– подбор логина и пароля в интерактивном режиме;

– подсматривание за пользователем при вводе им данных;

– преднамеренную передачу пароля его владельцем другому лицу;

– захват базы данных системы парольной защиты (если пароли не хранятся в базе в открытом виде, для их восстановления может потребоваться подбор или расшифрование);

– перехват переданной по сети информации в процессе аутентификации субъекта доступа;

– хранение пароля в доступном для нарушителя месте.

2. Вмешательство в функционирование компонентов системы парольной защиты через:

– внедрение вредоносной программы;

– обнаружение и использование ошибок, допущенных на стадии разработки системы;

– выведение из строя системы за счет создания условий, при которых в ней реализуется программный или технический сбой.

Пароль состоит из некоторого числа символов некого алфавита (A) и имеет определенную длину с количеством символов (L). Число всех возможных паролей (S) длиной L, которые можно составить из символов алфавита A, определяется следующим выражением:

$$S = A^L.$$

Одна из распространенных атак, позволяющих подобрать пароль, называется *brute force* (пер. с англ. «грубая сила»). Она заключается в переборе всевозможных комбинаций пароля при известной его длине.

Стойкость пароля к подобным атакам определяется его энтропией (степенью неопределенности). Чем выше энтропия пароля, тем больше вре-

мени потребуется нарушителю для его подбора. Энтропия пароля определяется в соответствии со следующим выражением:

$$H = L \cdot \frac{\log A}{\log 2}.$$

В соответствии с выражением можно утверждать, что энтропия пароля, а соответственно и его стойкость, будет в большей степени определяться его длиной.

Перебор паролей нарушитель проводит с использованием средств вычислительной техники, которые характеризуются некоторой производительностью. Чем больше производительность, тем меньше времени необходимо для подбора пароля. Кроме того, пароль можно с некоторой периодичностью менять, что также будет влиять на сложность его подбора нарушителем.

В результате чего можно рассчитать вероятность подбора нарушителем пароля:

$$P = \frac{V \cdot T}{A^L},$$

где V – скорость подбора пароля нарушителем;

T – максимальный срок действия пароля.

Отсюда можно выразить значение нижней границы всевозможных паролей (S^*) при соответствующих известных значениях:

$$S^* = \frac{V \cdot T}{P}.$$

Это значение позволяет определить длину пароля и его алфавит, при которых вероятность подбора пароля будет равна заданной.

Предположим, что $P = 10^{-6}$, $T = 7$ дней, $V = 10$ паролей/мин. Перед расчетом необходимо привести исходные данные, касающиеся времени, к единой временной единице.

Поэтому $V = 10$ паролей/мин $= 10 \cdot 60 \cdot 24 \cdot 7 = 100800$ паролей в неделю. Тогда

$$S^* = \frac{100800 \cdot 1}{10^{-6}} = 1008 \cdot 10^8 \text{ комбинаций паролей.}$$

Учитывая, что $S^* \le S = A^L$, необходимо предъявить следующие требования к паролю: $A = 26$, $L = 8$. Указанному A соответствует латинский алфавит, состоящий из малых букв.

Необходимо помнить, что одно из важнейших требований, предъявляемых к паролю, – это хранение его в секрете. Это означает, что пароль должен быть таким, чтобы, с одной стороны, его мог запомнить пользователь, а с другой – сохранялась стойкость в пределах определенного временного интервала. В организациях требования к паролю определяются политикой парольной защиты, которая является внутриведомственным нормативным правовым актом.

Практическое задание

1. Определите минимальное количество символов в пароле и минимальную его длину при заданных значениях вероятности его подбора, максимального срока его действия и скорости подбора пароля нарушителем, в соответствии с вариантом задания (табл. 7.1), которое задается преподавателем. На основании полученных результатов расчета определите состав удовлетворяющего полученным данным алфавита.

2. Используя ресурс *www.2ip.ru* (меню «Стойкость пароля»), определите время подбора каждого из паролей длиной 8 символов, состоящих:

1) из малых букв латинского алфавита;

2) одинаковых букв латинского алфавита;

3) малых букв русского алфавита;

4) одинаковых букв русского алфавита.

Сделайте вывод по результатам данного задания.

3. Используя ресурс *www.2ip.ru* (меню «Стойкость пароля»), определите минимальную длину пароля, при котором его стойкость будет обеспечиваться не менее 1 года:

1) для русского алфавита;

2) для латинского алфавита.

4. Используя ресурс *www.2ip.ru* (меню «Стойкость пароля») и данные, полученные при выполнении задания 2, составьте пароль, который имеет не меньшую стойкость, чем в задании 3, но меньшую длину:

1) при условии, что основу его составляет русский алфавит;

2) при условии, что основу его составляет латинский алфавит.

Таблица 7.1

Исходные данные для выполнения расчета

Вариант	P	V	T
1	10^{-2}	10 паролей/мин	5 дней
2	10^{-3}	100 паролей/мин	1 неделя
3	10^{-4}	1000 паролей/мин	2 недели
4	10^{-5}	10000 паролей/мин	3 недели
5	10^{-6}	11000 паролей/мин	1 месяц
6	10^{-7}	10 паролей/сек	2 месяца
7	10^{-2}	100 паролей/сек	3 месяца
8	10^{-3}	1000 паролей/сек	4 месяца
9	10^{-4}	10000 паролей/сек	5 месяца
10	10^{-5}	11000 паролей/сек	5 дней
11	10^{-6}	12000 паролей/сек	1 неделя
12	10^{-7}	10 паролей/день	2 недели
13	10^{-2}	100 паролей/день	3 недели
14	10^{-3}	1000 паролей/день	1 месяц
15	10^{-4}	10000 паролей/день	2 месяца

Контрольные вопросы

1. Что такое система авторизации?
2. Что такое субъект доступа?
3. Дайте характеристику всем видам идентификаторов.
4. Какие особенности реализации угроз в системах парольной защиты?
5. Какие требования предъявляются к паролю?

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 8: «ОЦЕНКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Цель занятия: изучить методику оценки рисков информационной безопасности и получить практические навыки по ее применению.

Краткие теоретические сведения

Необходимость обеспечения безопасности информации определяется тем ущербом, который может быть нанесен вследствие ее утечки. В случае если ущерб не является приемлемым, то необходимо его минимизировать за счет использования методов и реализующих их средств защиты информации. Их применение, особенно в информационных системах, требует определения некоторого показателя, который бы позволил оценить эффективность их использования. Данный критерий носит наименование риска информационной безопасности.

Сущность минимизации риска информационной безопасности сводится к получению такого значения остаточного риска, которое является приемлемым для организации. Для того чтобы обеспечить этот процесс, необходимо управлять рисками информационной безопасности, что реализуется в соответствии с моделью (рис. 8.1).

Владелец информационного ресурса (в соответствии с законодательством Республики Беларусь – руководитель организации) стремится его защитить от несанкционированного доступа (утечка информации в информационных системах). Для этого он использует определенные контрмеры (средства защиты информации), которые позволяют обеспечить снижение риска потери информационного ресурса. Такое стечение обстоятельств усложняет задачу несанкционированного доступа нарушителя к информации и, соответственно, минимизирует риск потери информационного ресурса его владельцем.

Для того чтобы нарушителю получить несанкционированный доступ в таких условиях, ему необходимо найти уязвимость в системе защиты, которая позволит ему достичь цели.

Уязвимость – возможность возникновения на каком-либо этапе жизненного цикла информационной системы такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.

Таким образом, минимизация риска обусловлена рядом факторов: устранением уязвимостей в информационных системах и использованием средств защиты информации.

Рис. 8.1. Модель управления рисками информационной безопасности

Оценка рисков информационной безопасности выполняется в соответствии с нижеприведенной методикой.

Этап 1. Определяется состав информационных активов информационной системы и ее границы (оборудование, входящее в нее).

Информационный актив – информация вне зависимости от формы ее представления, использование которой в процессе производственной деятельности позволяет организации получать прибыль.

Этап 2. Определяется стоимость информационных активов. Это позволяет оценить их значимость для организации и стоимость их утраты, а также определить необходимость и достаточность предлагаемых средств их защиты.

Этап 3. Оцениваются угрозы безопасности информации и уязвимости информационной системы, посредством которых они могут быть реализованы.

Это приводит к следующим возможным **последствиям**:

Последствие 1. Ущерб репутации организации.

Последствие 2. Финансовые потери, связанные с восстановлением информационных активов.

Последствие 3. Невозможность деятельности компании вследствие нарушения функционирования ее информационной системы.

Последствие 4. Финансовые потери от разглашения и передачи информации третьим лицам.

Этап 4. Выполняется анализ рисков информационной безопасности, что позволяет оценить потери организации вследствие реализации угроз безопасности информации. Оценка риска информационной безопасности по двум факторам: вероятность возникновения угрозы безопасности информации и цена ущерба – выполняется с использованием следующего выражения:

$$\text{РИСК} = \text{ВЕРОЯТНОСТЬ}_{\text{УГР}} \cdot \text{ЦЕНА}_{\text{УЩ}}.$$

Оценка риска информационной безопасности по трем факторам: вероятность возникновения угрозы безопасности информации, вероятность использования нарушителем некоторой уязвимости, что приводит к реализации некоторой угрозы, и цена ущерба – выполняется с использованием следующего выражения:

$$\text{РИСК} = \text{ВЕРОЯТНОСТЬ}_{\text{УГР}} \cdot \text{ВЕРОЯТНОСТЬ}_{\text{УЯЗВ}} \cdot \text{ЦЕНА}_{\text{УЩ}}.$$

Если информационный актив подвержен нескольким (N) угрозам безопасности информации, то общий риск $\text{РИСК}_{\text{общ}}$ нанесения нарушителем ущерба может быть определен как

$$\text{РИСК}_{\text{общ}} = \sum_{i=1}^{N} p_i \cdot U_i ,$$

где p_i – $\text{ВЕРОЯТНОСТЬ}_{\text{ущ}}$ (весовой коэффициент) i-й угрозы, выбираемая экспертами из условия $\sum_{i=1}^{N} p_i = 1$;

U_i – $\text{ЦЕНА}_{\text{ущ}}$ по i-й угрозе.

Этап 5. Реализуется управление рисками. На этом этапе выбираются средства защиты информации, которые позволят снизить риск.

При анализе риска информационной безопасности используют следующие термины.

Критичность реализации угрозы (ER) – степень влияния угрозы безопасности информации на информационный актив (конфиденциальность, целостность, доступность, сохранность, подлинность).

Вероятность реализации угрозы безопасности информации через определенную уязвимость (P (V)) определяет вероятность реализации угрозы безопасности информации через определенную уязвимость информационной системы.

Учитывая эти термины, определяется уровень угрозы по уязвимости (*Th*):

$$Th = \frac{ER}{100} \cdot \frac{P(V)}{100}.$$

На основании значений уровня угрозы по уязвимости осуществляется расчет по всем уязвимостям, по которым реализуется данная угроза (*CTh*):

$$CTh = 1 - \prod_{i=1}^{n} (1 - Th_n).$$

Рассмотрим пример. Пусть проводится оценка рисков информационной безопасности следующей информационной системы (рис. 8.2).

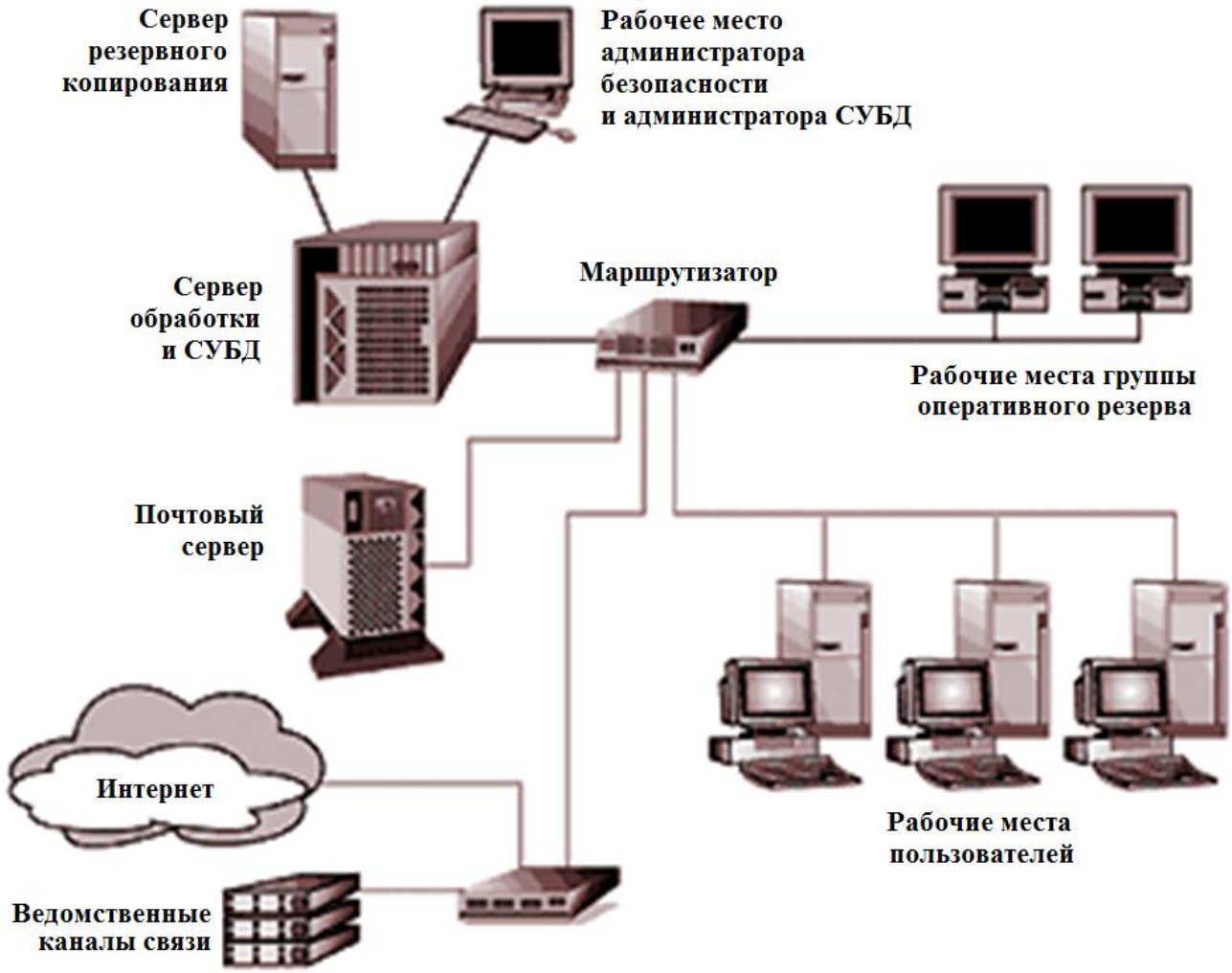


Рис. 8.2. Архитектура информационной системы

Как видно из рис. 8.2, архитектура информационной системы следующая:

– рабочие места (РМ) ввода информации – персональные компьютеры, на которых пользователи обрабатывают информацию;

– почтовый сервер, на который информация поступает с удаленных узлов сети через сеть Интернет и по ведомственным каналам связи (ВКС);

– сервер обработки информации и система управления базами данных (СУБД) используются для хранения информации в базе данных, взаимодействие пользователей с которой осуществляется через СУБД;

– сервер резервного копирования предназначен для хранения резервных копий базы данных и ее восстановления в случае сбоя сервера обработки и СУБД;

– рабочие места группы оперативного резерва – персональные компьютеры, на которых пользователи обрабатывают информацию в случае выхода из строя рабочих мест ввода информации;

– рабочее место администратора безопасности и администратора СУБД – персональный компьютер, предназначенный для настройки и технической эксплуатации информационной системы.

Функционирование информационной системы осуществляется следующим образом. Данные, введенные с РМ пользователей, поступившие на почтовый сервер из сети Интернет и из ВКС, направляются на сервер обработки данных и СУБД.

Практическое задание

Проанализируем риски информационной безопасности информационных активов информационной системы (табл. 8.1) с помощью вышеизложенной методики.

Этап 1. Определение границ информационной системы. Для этого определим состав информационных. Допустим, что информационными активами являются следующие:

Актив 1. Данные, поступившие на сервер обработки и СУБД из сети Интернет.

Актив 2. Данные, поступившие на сервер обработки и СУБД из ВКС.

Актив 3. Данные, поступившие на сервер обработки и СУБД с РМ пользователей.

Актив 4. Системное и прикладное программное обеспечение.

Актив 5. Данные, хранимые в базе данных.

Этап 2. Определение стоимости информационных активов. Сведения о стоимости информационных активов представлены в табл. 8.1.

Таблица 8.1

Стоимость информационных активов

Наименование актива	Актив 1	Актив 2	Актив 3	Актив 4	Актив 5
Стоимость актива, тыс. р.	7	5	32	1000	50 000

Этап 3. На основании анализа особенностей обработки информации в информационной системе определены следующие угрозы безопасности информации:

Угроза 1. Загрузка из сети Интернет в информационную систему вредоносной программы, обусловленная непреднамеренными действиями сотрудника организации.

Угроза 2. Передача информации сотрудником организации, который имеет к ней легальный доступ, третьим лицам.

Этап 4. Пусть в результате реализации *угрозы 1* с вероятностью 0,6 наступило последствие «Финансовые потери, связанные с восстановлением информационных активов». Вредоносная программа загружалась в информационную систему 6 раз за год и каждый раз повреждала на 100 % *активы 1–3* и на 30 % *актив 4*, что обуславливает критичность реализации *угрозы 1* через *уязвимость 1*, обусловленную недостатками технологий управления активами этой информационной системы. *Актив 5* был защищен резервным копированием, поэтому его повреждением можно пренебречь.

Кроме того, в результате реализации этой угрозы наступило последствие «Невозможность деятельности компании вследствие нарушения функционирования ее информационной системы». Пусть за 6-кратную в течение года загрузку вредоносной программы цена ущерба по этому последствию составила 21 тыс. р.

В результате реализации *угрозы 2* с вероятностью 0,4 наступило последствие «Финансовые потери от разглашения и передачи информации третьим лицам». Пусть цена ущерба составила 56 тыс. р.

Кроме того, в результате реализации этой угрозы наступило последствие «Ущерб репутации организации». Пусть цена ущерба за счет уменьшения потока заказов составила 88 тыс. р.

Этап 5. Выбор методов и средств минимизации угроз. Для противодействия *угрозе 1* необходимо использовать средство защиты информации – антивирусное программное средство, а для противодействия *угрозе 2* – разработать и внедрить систему парольной защиты для доступа к информационным активам организации. Стоимость лучшего по техническим параметрам антивирусного программного средства – 90 тыс. р. Стоимость разработки и внедрения лучшей системы парольной защиты – 20 тыс. р. Утвержденный годовой бюджет на информационную безопасность в организации составляет 80 тыс. р. Для принятия решения о рациональном распределении финансовых средств необходимо выполнить оценку рисков.

Задание 1. Найти цену ущерба при реализации *угрозы 1*.

Задание 2. Найти цену ущерба при реализации *угрозы 2*.

Задание 3. Найти общий риск при реализации *угрозы 1* и *угрозы 2*.

Задание 4. Исходя из размера выделенного годового бюджета на информационную безопасность в организации, необходимо минимизировать остаточный риск информационной безопасности за счет оптимального распределения средств (80 тыс. р.) на противодействие *угрозе 1* и противодействие *угрозе 2*,

считая, что для рассматриваемой информационной системы экспертным путем установлено, что:

– недостаток каждых x % средств от стоимости лучшего антивирусного программного средства позволяет приобрести менее дорогое антивирусное программное средство; однако это обуславливает риск реализации угрозы безопасности информации, исчисляемый в денежном эквиваленте, в размере

$$584,4 \cdot \frac{x}{100} \text{ [тыс. р.];}$$

– недостаток каждых y % средств от стоимости лучшей системы парольной защиты позволяет приобрести менее дорогую систему; однако это обуславливает риск реализации угрозы безопасности информации, исчисляемый в денежном эквиваленте, в размере

$$141,6 \cdot \frac{y}{100} \text{ [тыс. р.].}$$

Задание 5. Оценить эффективность принятых мер для противодействия угрозам безопасности информации по формуле

$$E = \frac{\text{РИСК}_{\text{ОБЩ}} - \text{РИСК}_{\text{ОСТАТ}}}{\text{РИСК}_{\text{ОБЩ}}} \cdot 100\,\%.$$

Задание 6. Найти критичность реализации *угрозы 1* через *уязвимость 1*. Определить для всех отмеченных выше угроз и уязвимостей *Th* и *CTh*, если критичность реализации *угрозы 1* через *уязвимость 2* составляет 20 %; *угрозы 2* через *уязвимость 1* – 40 %; *угрозы 2* через *уязвимость 2* – 30 %. Реализацию угроз безопасности информации через каждую из уязвимостей считать равновероятной.

Контрольные вопросы

1. В чем заключается сущность минимизации риска информационной безопасности?
2. За счет чего можно минимизировать риск информационной безопасности?
3. Что такое информационный актив?
4. Каким образом оценивается риск?
5. Что является критерием эффективности принятых мер для противодействия угрозам безопасности информации?

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Пулко, Т. А. Введение в информационную безопасность : учеб. пособие / Т. А. Пулко. – Минск : БГУИР, 2016. – 164 с.

2. Новиков, В. К. Информационная безопасность и защита информации : организационно-правовые основы / В. К. Новиков, И. Б. Галушкин, С. В. Аксёнов. – М. : Горячая линия-Телеком, 2016. – 312 с.

3. Петраков, А. В. Основы практической защиты информации : учеб. пособие / А. В. Петраков. – 4-е изд. – М. : СОЛОН-пресс, 2005. – 384 с.

4. Мельников, В. П. Информационная безопасность и защита информации : учеб. пособие / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. – 3-е изд. – М. : Академия, 2008. – 336 с.

Св. план 2023, поз. 27

Учебное издание

Борботько Тимофей Валентинович
Бойправ Ольга Владимировна

МЕТОДОЛОГИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. ПРАКТИКУМ

УЧЕБНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ

Редактор *Ю. В. Ляховец*
Корректор *Е. Н. Батурчик*
Компьютерная правка, оригинал-макет *Е. Г. Бабичева*

Подписано в печать 08.04.2024. Формат 60×84 1/16. Бумага офсетная. Гарнитура «Таймс».
Отпечатано на ризографе. Усл. печ. л. 3,6. Уч.-изд. л. 4,0. Тираж 50 экз. Заказ 141.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники».
Свидетельство о государственной регистрации издателя, изготовителя,
распространителя печатных изданий №1/238 от 24.03.2014,
№2/113 от 07.04.2014, №3/615 от 07.04.2014.
Ул. П. Бровки, 6, 220013, г. Минск